Tight Multi-User Security of CCM and Enhancement by Tag-Based Key Derivation

Yusuke Naito[1], Yu Sasaki[2,3], and Takeshi Sugawara[4]

[1] Mitsubishi Electric Corporation, Kanagawa, Japan,
Naito.Yusuke@ce.MitsubishiElectric.co.jp
[2] NTT Social Informatics Laboratories, Tokyo, Japan, yusk.sasaki@ntt.com
[3] Associate of National Institute of Standards and Technology, Gaithersburg, US,
[4] The University of Electro-Communications, Tokyo, Japan, sugawara@uec.ac.jp

Abstract. This paper studies the multi-user (mu) bound of Counter with CBC-MAC (CCM), the authenticated encryption mode for block ciphers (BCs). Galois/Counter Mode (GCM) is more advanced in the study of mu security, and Hoang et al. achieved the tight mu-security bound of $\frac{\sigma_u \sigma}{2^n} + \frac{up+u^2}{2^k}$, where k and n are respectively the key and block sizes, u is the number of users, p is the number of offline queries. Here, σ and σ_{u} are the crucial factors that represent the total number of BC invocations by all users and the maximum number of BC invocations per user, respectively. In contrast, while there are two known mu bounds for CCM, $\frac{u\sigma_{\mathsf{u}}^2}{2^n} + \frac{up+u^2}{2^k}$ by Luykx et al. (Asiacrypt 2017) and $\frac{\sigma^2}{2^n} + \frac{up+u\sigma}{2^k}$ by Zhang et al. (CCS 2024), both of which are not tight and worse than the bound for GCM. Another line of research studies methods to enhance mu-security without disruptive changes, such as nonce randomization (NR) and nonce-based key derivation (NKD) to improve offline and online security, respectively, but their applicability to CCM has never been discussed. Filling these gaps, this paper first proves an improved mu-security bound of CCM, which is tight, and reaches the GCM's bound. We also prove that CCM combined with NR and NKD achieves the same bound as GCM. With these results, CCM is now proved to be as secure as GCM. Furthermore, we propose a new enhancement method called nonce-based and tag-based key derivation (NTKD) and apply it to GCM and CCM. NTKD achieves a better bound beyond NR and NKD, and the resulting schemes satisfy the needs of real-world applications that demand massive data.

Keywords: CCM · Multi-user Security · Security Proof · Improved Bound · Nonce Randomization · Nonce/Tag-based Key Derivation

1 Introduction

Privacy and message authenticity are two fundamental properties required for secure and reliable information systems. Real-world systems widely deploy authenticated encryption (AE), a symmetric-key cryptosystem that provides both

privacy and authenticity, and researchers are actively studying their provable security bounds to provide theoretical foundation for determining their operational parameters, such as the frequency of changing a key.

Galois/Counter Mode (GCM) and Counter with CBC-MAC (CCM) are popular ways of constructing AE schemes based on a block cipher (BC) and a message authentication code (MAC). GCM uses the counter (CTR) mode for encryption and a polynomial hash function for MAC. GCM is standardized as ISO/IEC 19772 [15] and NIST SP800-38D [9] and widely used in many practical protocols, including Ethernet security [30], WPA3 Wifi security protocol [35], IPSec [32], and TLS [29]. CCM, on the other hand, uses the CTR mode for encryption and the cipher block chaining MAC (CBC-MAC) for MAC. It is standardized in IEEE 802.11 standard for wireless LANs [33, 28], RFC 3610 [34], and NIST SP800-38C [8] and widely deployed in ZigBee [38], IPSec [14, 4], Bluetooth [36], and TLS 1.3 defined in 2018 [26, 20].

Conventionally, the security of AE schemes has been proved and analyzed based on the single-user (su) model that considers a single user with a fixed key. Missing consideration of an attack targeting a service with many users is a considerable gap, and there is a demand for rigorous security evaluation with the multi-user (mu) model, which considers an attacker who tries to compromise any of multiple users. Addressing the issue, researchers have evaluated several AE schemes in the last few years, including AES-GCM [2, 13, 19], AES-GCM-SIV [5], and ChaCha20-Poly1305 [7]. Based on those results, major protocols, such as TLS, DTLS, and QUIC, determine the rekeying intervals of AES-GCM according to the mu-security limit [26, 27, 31]. Moreover, the ongoing discussion on the usage limit of AEs, published as Internet-Draft [12], considers mu-security for other schemes, including AES-CCM.

Hoang et al. [13] proved that GCM's mu-security bound is $\frac{\sigma_{\mathsf{u}}\sigma}{2^n}+\frac{q_{\mathsf{d}}}{2^t}+\mathbf{Adv}_E^{\mathsf{muprp}}$, where E is the underlying BC, n and k are the block and key lengths of E, t is the tag length, and $\mathbf{Adv}_E^{\mathsf{muprp}}$ is the mu-pseudorandom-permutation (mu-PRP) advantage of E. σ is the total BC invocations in online queries, i.e., the queries to the encryption and decryption oracles, and σ_{u} is the upper bound of the number of BC invocations in online queries for each user, and q_{d} is the number of decryption queries. Note that Table 1 summarizes the parameters included in the bounds that appear throughout the paper. Assuming that $\frac{q_{\mathsf{d}}}{2^t} \leq \frac{\sigma_{\mathsf{u}}\sigma}{2^n}$, the bound matches the collision finding attack on CTR and is tight regarding online security.[5]

In contrast, mu-security of CCM is relatively unclear compared to GCM. Jonsson [17] proved that CCM's su-security bound in the ideal cipher (IC) model is $\frac{\sigma^2}{2^n}+\frac{q_{\mathsf{d}}}{2^t}+\frac{p}{2^k}$, wherein p is the number of offline queries to IC. The aforementioned Internet-Draft document [12] evaluates mu-security of AES-CCM with a generic bound, i.e., an mu-bound obtained from an su-bound with a hybrid argument,

[5] The adversary has access to u users and makes encryption queries such that all plaintexts are zero strings and the number of plaintext blocks per user is σ_{u}, thus $\sigma = u\sigma_{\mathsf{u}}$. Since no collision occurs in the BC's outputs within the same user, the birthday analysis offers the distinguishing probability $\Omega(\frac{u\sigma_{\mathsf{u}}^2}{2^n}) = \Omega(\frac{\sigma_{\mathsf{u}}\sigma}{2^n})$.

Table 1. Parameters that appear in the bounds.

Parameter	Description
E	Underlying block cipher
n	Block length of E
k	Key length of E
t	Tag length
u	Number of users
p	Number of offline queries to an ideal cipher
d	The number of the same nonces across distinct keys
σ	Total number of BC invocations in online queries
σ_{u}	The number of BC invocations for each user
σ_{n}	The number of BC invocations for each nonce in a single user
q_{d}	Number of decryption queries
v	Threshold by implementing lockdown with failed decryption attempts

Table 2. Mu-bounds of GCM, CCM, and their enhancements with NR and NKD. For NKD, the mu-PRF advantage of KDF is omitted in this table, since it can be negligible by choosing a KDF and its key length appropriately.

Target	Bound	Ref.	Target	Bound	Ref.
GCM	$\frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{up+u^2}{2^k}$	[13]	CCM	$\frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{up+u^2}{2^k}$	Ours
+NR	$\frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{dp}{2^k}$	[13]	+NR	$\frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{dp}{2^k}$	Ours
+NR, NKD	$\frac{\sigma_{\mathsf{n}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{dp}{2^k}$	[13]	+NR, NKD	$\frac{\sigma_{\mathsf{n}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{dp}{2^k}$	Ours
CCM	$\frac{u\sigma^2}{2^n} + \frac{uq_{\mathsf{d}}}{2^t} + \frac{up+u\sigma}{2^k}$	Generic	Tag-based AE	$\frac{\sqrt{\sigma_{\mathsf{n}}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{dp}{2^k}$	Ours
CCM	$\frac{u\sigma_{\mathsf{u}}^2}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{up+u^2}{2^k}$	[19]	+NR, NTKD		
CCM	$\frac{\sigma^2}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{up+u\sigma}{2^k}$	[37]			

given by $\frac{u\sigma^2}{2^n} + \frac{uq_{\mathsf{d}}}{2^t} + \frac{up+u\sigma}{2^k}$. Such a generic bounds degrades with the number of users u, and further improvement with dedicated proofs is a significant research challenge [19, 37]. Luykx et al. [19] showed a condition on deriving an mu-bound from an su-bound without security degradation, providing the improved mu-bound of CCM, given by $\frac{u\sigma_{\mathsf{u}}^2}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \mathbf{Adv}_E^{\mathsf{muprp}}$ wherein $\mathbf{Adv}_E^{\mathsf{muprp}}$ is bounded by $\frac{up+u^2}{2^k}$ in the IC model.

Zhang et al. [37] showed another mu-bound of CCM, which is $\frac{\sigma^2}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{up+u\sigma}{2^k}$. They showed the tightness of the bound under some conditions. The second term $\frac{q_{\mathsf{d}}}{2^t}$ is tight with generic forgery attacks that exhaustively guess the tags. The third term $\frac{up+u\sigma}{2^k}$ corresponds to attacks with offline queries, and this is tight when the offline query overwhelms the online query, i.e., $\sigma \leq p$. In contrast, the first term $\frac{\sigma^2}{2^n}$ is proved to be tight only in the extreme case with $\sigma_{\mathsf{u}} \approx \sigma$, i.e., an adversary sends all online queries to a single user. This case is essentially equivalent that

the adversary performs an su-attack even the access to multi-users is given, thus it does not demonstrate truly meaningful tightness w.r.t. mu-security.

Significance between $\frac{u\sigma_{\mathsf{u}}^2}{2^n}$ and $\frac{\sigma^2}{2^n}$ depends on the parameters u, σ_{u}, and σ; Zhang et al.'s $\frac{\sigma^2}{2^n}$ is better than Luykx et al.'s $\frac{u\sigma_{\mathsf{u}}^2}{2^n}$ in the extreme cases with $u \approx \sigma$ (e.g., $\sigma_{\mathsf{u}} = \sigma^{3/4}$ and $u \approx \sigma$), but Zhang et al's bound is worse in other cases, such as $\sigma \approx u\sigma_{\mathsf{u}}$, i.e. each of u users is queried with σ_{u} BC invocations. However, both bounds have critical problems. Zhang et al.'s $\frac{\sigma^2}{2^n}$ indicates that CCM's security is broken when σ reaches the birthday bound, and this cannot be avoided no matter how strong limitations are imposed on each user. Luykx et al's $\frac{u\sigma_{\mathsf{u}}^2}{2^n}$ only considers the maximum BC invocation per user, and thus non-tight when data from some users do not reach the maximum. Moreover, both bounds are worse than GCM's mu-bound of $\frac{\sigma_{\mathsf{u}}\sigma}{2^n}$ [13].

Another line of research work aims to enhance the security without disruptive changes in the scheme. For example, both GCM's and CCM's mu-offline security is already tight bounded by Biham's attack [3], which lowers the amount of offline queries to $\frac{2^k}{u}$, and there is no room for improvement as long as GCM's and CCM's specification are maintained. GCM in TLS 1.3 implements a countermeasure called nonce randomization (NR) that preprocesses the nonce without changing the GCM's implementation interface. NR uses a randomized nonce $N_{\mathrm{rand}} = N_{\mathrm{orig}} \oplus R$ with the original ν-bit nonce N_{orig} and a user-specific random mask $R \in \{0,1\}^\nu$. With this modification, Biham's attack additionally requires a collision in N_{rand} and the offline security is improved from $\frac{2^k}{u}$ to 2^k.

Bellare and Tackmann [2] proved confidentiality of NR, but the analysis is merely non-tight and did not consider integrity. Hoang et al. [13] formalized NR by introducing the d-bound model, where the number of the same randomized nonces across distinct users is bounded by d;[6] in the d-bound and the IC models, the new mu-bound of GCM with NR becomes $\frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{dp}{2^k}$, as summarized in Table 2.

Nonce-based key derivation (NKD) [11] is another method that enhances online (cf. offline) security. Note that NKD is a meaningful technique for real-world applications, and in fact, NIST recently announced their interest in revising NIST SP800-38D to standardize the combination of GCM and NKD [23]. In NKD, each pair of a randomized nonce and a key for key derivation function (KDF) generates a fresh key of an AE scheme, and combining it with the mu-bound in the d-bound model provides the following mu-bound of GCM with NKD, $\frac{\sigma_{\mathsf{n}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{dp}{2^k} + \mathbf{Adv}_{\mathsf{F}}^{\mathsf{muprf}}$, where σ_{n} is the maximum number of BC invocations per nonce in a single user and $\mathbf{Adv}_{\mathsf{F}}^{\mathsf{muprf}}$ is an mu-pseudorandom-function (mu-PRF) advantage of the KDF F. Note that $\mathbf{Adv}_{\mathsf{F}}^{\mathsf{muprf}}$ can be negligible by choosing a KDF and its key length appropriately. Since $\sigma_{\mathsf{n}} \leq \sigma_{\mathsf{u}}$, NKD enhances the security of GCM. In particular, we can significantly improve security by limiting the number of decryption failures to some constant, i.e., $\sigma_{\mathsf{n}} \ll \sigma_{\mathsf{u}}$.

[6] As a principle of nonce respect, the same (randomized) nonce is never repeated with the same key. However, the same nonce may appear between different users, and it is necessary to evaluate the number of nonce repetitions across distinct users.

Table 3. Upper-bounds of BC invocations for online mu-security with concrete parameters: $n = 128$ and several per-user usage limits, (i) $\sigma_{\mathsf{u}} = 2^{34.5}$, (ii) $\sigma_{\mathsf{u}} = 2^{48}$, and (iii) $\sigma_{\mathsf{u}} = 2^{53}$, from practical standards. σ_{n} is upper-bounded by about $v\ell$ and this table evaluates σ for $v = 2^{10}$ and $\ell = 2^{24}$. We approximate that $k - \log_2 d \approx k$.

Target	Online				Offline
	Generic	$\sigma_{\mathsf{u}} = 2^{34.5}$	$\sigma_{\mathsf{u}} = 2^{48}$	$\sigma_{\mathsf{u}} = 2^{53}$	Generic
CCM [37]	$\sigma \le 2^{n/2}$	$\sigma \le 2^{64}$	$\sigma \le 2^{64}$	$\sigma \le 2^{64}$	$k - \log_2 u$
CCM	$\sigma \le \frac{2^n}{\sigma_{\mathsf{u}}}$	$\sigma \le 2^{93.5}$	$\sigma \le 2^{80}$	$\sigma \le 2^{75}$	$k - \log_2 u$
CCM w/ NR	$\sigma \le \frac{2^n}{\sigma_{\mathsf{u}}}$	$\sigma \le 2^{93.5}$	$\sigma \le 2^{80}$	$\sigma \le 2^{75}$	k
CCM w/ NR + NKD	$\sigma \le \frac{2^n}{\sigma_{\mathsf{n}}}$	$\sigma \le 2^{94}$			k
GCM/CCM w/ NR + NTKD	$\sigma \le \frac{2^n}{\sqrt{\sigma_{\mathsf{n}}}}$	$\sigma \le 2^{111}$			k

So far, enhancing methods such as NR and NKD have only been discussed for GCM, but their applicability to CCM has never been discussed. CCM is far behind GCM also in this respect.

It is also necessary to consider whether the enhanced security by NR and NKD is sufficient. The offline security term $\frac{dp}{2^k}$ is almost tight, because $k - \log_2 d \approx k$. Hence, possible concerns are on online security. Amazon AWS showed that AE schemes should allow to encrypt 2^{92} messages [18]. By combining it with the limitation of TLS 1.3 [26] that the maximum size of each message, ℓ, is 2^{10} blocks, AE schemes must be secure for $\sigma = 2^{102}$ BC invocations. Let us assume that the BC is AES having $n = 128$. With the original GCM and only with NR, the online term is $\frac{\sigma_{\mathsf{u}}\sigma}{2^{128}}$. TLS 1.3 [26] limits $\sigma_{\mathsf{u}} = 2^{34.5}$ BC invocations in AES-GCM,[7] and the aforementioned Internet Draft document [12] is establishing similar limits for other schemes. NIST standards have the same kind of limits: NIST SP800-38B for CMAC [10] recommends $\sigma_{\mathsf{u}} = 2^{48}$ BC invocations when $n = 128$, and NIST SP800-38D for AES-GCM [9] limits $\sigma_{\mathsf{u}} = 2^{53}$ BC invocations.[8] Even with the strongest limitation of $\sigma_{\mathsf{u}} = 2^{34.5}$ by TLS 1.3, the maximum σ is $2^{93.5}$ as shown in Table 3, which does not reach the goal of 2^{102}. When NKD is used, the online term is $\frac{\sigma_{\mathsf{n}}\sigma}{2^{128}}$. Adversaries can make queries under the same nonce up to v, the number of acceptable verification failures in decryption, hence σ_{n} is upper-bounded by about $v\ell$. To ensure security for $\sigma = 2^{102}$ with $\ell = 2^{24}$ coming from the maximum counter size of CCM, v can be at most 4. Practical systems can limit v to a constant threshold by implementing lockdown with failed decryption attempts, however $v = 4$ is too strong limitation, which significantly lowers usability.

[7] $2^{34.5}$ is derived from the maximum number of messages ($2^{24.5}$) and $\ell = 2^{10}$ blocks.

[8] NIST SP800-38D [9] tolerates 2^{21} messages for each key with 96-bit IV and 2^{32} blocks per message restricted by the counter length, totaling 2^{53} blocks for each key.

Table 4. Key generation methods and nonce generation methods of CCM/GCM, NKD, NTKD, and NR. K_{AE} and N_{AE} are a key and nonce of CCM/GCM, respectively. N_{orig} is an original nonce input to the target AE. $K_{\mathsf{AE}} \xleftarrow{\$} \{0,1\}^n$ means that K_{AE} is chosen uniformly at random from $\{0,1\}^k$. F_K is a KDF with a key K. For NR, R is a per-user fixed random value with the same length as N_{AE}. For NTKD, i is the sector number and T_{i-1} is a tag of the previous AE call.

Target	AE's Key Generation	Target	AE's Nonce Generation
CCM/GCM	$K_{\mathsf{AE}} \xleftarrow{\$} \{0,1\}^n$	CCM/GCM	$N_{\mathsf{AE}} \leftarrow N_{\mathrm{orig}}$
+NKD	$K_{\mathsf{AE}} \leftarrow \mathsf{F}_K(N_{\mathrm{orig}})$	+NR	$N_{\mathsf{AE}} \leftarrow N_{\mathrm{orig}} \oplus R$
+NTKD	$(K_{\mathsf{AE}}, *) \leftarrow \mathsf{F}_K(N_{\mathrm{orig}}, T_{i-1})$	+NTKD	$(*, \hat{N}) \leftarrow \mathsf{F}_K(N_{\mathrm{orig}}, 0^t)$; $N_{\mathsf{AE}} \leftarrow \hat{N} + (i-1)$

In summary, mu-security of CCM still falls short compared to GCM in online security and the existing enhancements, as summarized in Table 2. Moreover, the existing enhancements may not be sufficient for some practical use cases. This paper aims to fill the gaps between CCM and GCM, and to present a new enhancement method to reach an ideal mu-security level. In particular, we address the following research questions: (1) What is the tight online mu-bound of CCM? Is it better or worse compared to GCM? (2) Do conventional enhancing methods, i.e., NR and NKD, improve mu-security of CCM? If yes, how much? (3) Is it possible to further enhance mu-security beyond NR and NKD, which works for both GCM and CCM?

Contributions

In the first part of this paper, we prove that CCM is as good as GCM with respect to mu-security for the standard model, NR, and NKD, with the following contributions. The generation methods of key and nonce for these schemes are summarized in Table 4.

Tight Mu-bound in the Standard Model (Section 5). We first improve the mu-bound of CCM in the standard model to $\frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \mathbf{Adv}_E^{\mathsf{muprp}}$. The first two terms $\frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t}$ represent the online security, which are better than the corresponding terms in the previous work, i.e., $\frac{\sigma^2}{2^n} + \frac{q_{\mathsf{d}}}{2^t}$ and $\frac{u\sigma_{\mathsf{u}}^2}{2^n} + \frac{q_{\mathsf{d}}}{2^t}$, for any adversary since $\sigma \leq u\sigma_{\mathsf{u}}$ and $\sigma_{\mathsf{u}} \leq \sigma$. The new online terms are tight, i.e. match the generic bounds of the distinguishing attack on CTR and a generic forgery attack. Furthermore, with condition $\sigma_{\mathsf{u}} \ll 2^{n/2}$, which can be ensured by adequate rekeying, CCM achieves beyond-birthday-bound online security. The offline security of CCM, on the other hand, is derived from the last term $\mathbf{Adv}_E^{\mathsf{muprp}}$. This mu-PRP term offers the bound $\frac{up+u^2}{2^k}$ in the IC model, which is also tight, matching the bounds of the generic attacks [3]. In summary, the entire bound is tight,

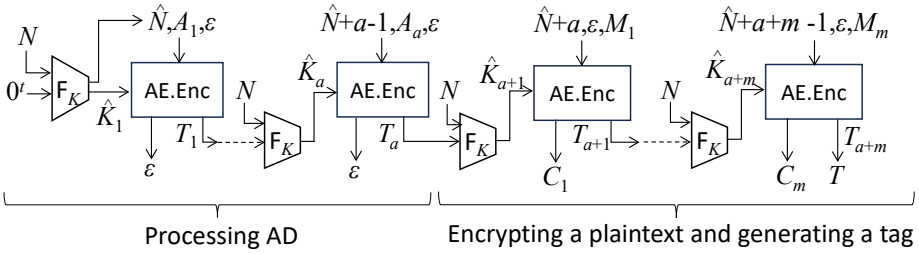

Fig. 1. Encryption of AE_NTKD. AE.Enc is the underlying tag-based AE encryption. F_K is the KDF that takes nonce and a tag and generates a key of AE.Enc (and a nonce-based IV $\hat{N}$ for the first AE.Enc call). $A_1, \ldots, A_a$ are AD sectors, $M_1, \ldots, M_m$ are plaintext sectors, $C_1, \ldots, C_m$ are ciphertext sectors, $T_1, \ldots, T_{a+m}$ are tags of AE.Enc, T is a tag of AE_NTKD. $\hat{N}$ with a counter addition is used as nonce of AE.Enc.

and CCM achieves the same level of mu security as GCM, as summarized in Table 2.

Enhancing Offline Security with NR (Section 6). Next, we prove that the mu-bound of CCM with NR in the d-bound and IC models is $\frac{\sigma_u \sigma}{2^n} + \frac{q_d}{2^t} + \frac{dp}{2^k}$. The last term $\frac{dp}{2^k}$ represents offline security, where d is $\approx \frac{n}{\log_2 n}$ and negligible. Thus, NR enhances offline security from $\frac{k}{u}$ to k bits, making it independent of the number of users. The online security represented by the first two terms, on the other hand, is identical to that of bare CCM in the standard model, which is tight. The bound is again the same as that of GCM in the d-bound and IC models, as shown in Table 2.

Enhancing Online Security with NKD (Section 7). While NR enhances the offline security of CCM, the online security remains unchanged with the term $\frac{\sigma_u \sigma}{2^n}$. We improve it using NKD, following the previous approach for GCM [13]. The mu-security of CCM with NKD in the d-bound and IC models is $\frac{\sigma_n \sigma}{2^n} + \frac{q_d}{2^t} + \frac{dp}{2^k} + \mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}$, obtained by replacing σ_u with σ_n and adding the mu-PRF advantage of F in the above mu-bound of CCM with NR. Although the mu-PRF advantage is added as a new offline term, it becomes negligible by choosing an appropriate KDF with sufficient key length, and the overall offline security is k bits.

The online security is enhanced under the condition that $\frac{\sigma_n \sigma}{2^n} \geq \frac{q_d}{2^t}$ and $\sigma_n \ll \sigma_u$. Because σ_n is upper-bounded by about $v\ell$, the online term is improved to about $\frac{v\ell\sigma}{2^n}$. The bound is the same as the one of GCM with NKD in the IC and d-bound models, thus CCM achieves the same level of mu security as GCM.

Nonce-Based and Tag-Based Key Derivation (NTKD) (Section 8). In the second part of this paper, we present a new method called NTKD to further

enhance online mu-security. NTKD can be applied to both GCM and CCM, and can be applied in generic for any tag-based AE: an AE such that (i) encryption generates a ciphertext C and a tag T and (ii) decryption generates T' without using T and authenticates the data by matching T and T'. The basic idea of NTKD is to separate the input data into multiple *sectors*, an appropriately parameterized number of data blocks, and apply AE to each sector by setting the key for the ith sector to an output of KDF that is computed from the nonce and the tag for $(i-1)$-th sector. The encryption of NTKD is depicted in Fig. 1 and the key generation method is given in Table 4. This has the effect of rekeying in every sector and improves security. By setting the sector length to $\sqrt{\sigma_{\mathsf{n}}}$, the mu-bound becomes $\frac{\sqrt{\sigma_{\mathsf{n}}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \frac{dp}{2^k}$. Because σ_{n} is upper-bounded by about $v\ell$, with $n = 128$, $\ell = 2^{24}$, and $\sigma = 2^{102}$, security is ensured as long as $v \leq 2^{28}$, which is significantly higher than $v \leq 4$ for NKD with the same setting. Also we evaluate the value of σ that can be securely processed for some v. with $n = 128$, $v = 2^{10}$, and $\ell = 2^{24}$, NTKD ensures security up to $\sigma = 2^{111}$, while NKD ensures security up to $\sigma = 2^{94}$, which does not reach $\sigma = 2^{102}$, as shown in Table 3.

Regarding the speed, the performance of NTKD depends on the plaintext length and the chosen sector length. The overhead may become significant with short plaintexts or small sector sizes; however, it becomes negligible for long plaintexts and appropriately chosen sector lengths, and NTKD achieves performance comparable to that of the original scheme.

2 Notations

Let ε be the empty string, $\emptyset$ the empty set, and $\{0,1\}^*$ the set of all bit strings. For integers $i \leq j$, let $[i,j] \coloneqq \{i, i+1, \ldots, j\}$ and $[j] := [1,j]$. If $i > j$ then $[i,j] \coloneqq \emptyset$. For an integer $n \geq 0$, let $\{0,1\}^n$ be the set of all n-bit strings, $\{0,1\}^0 \coloneqq \{\varepsilon\}$, $\{0,1\}^{\leq n} \coloneqq \cup_{i\in[0,n]}\{0,1\}^i$, and $\{0,1\}^{n*} \coloneqq \{X \in \{0,1\}^* \mid |X| > 0, |X| \bmod n = 0\}$. Let 0^i be the bit string of i-bit zeros. For a bit-string $D \in \{0,1\}^*$ and a positive integer n, let $|D|_n := \lceil |D|/n \rceil$ be the n-bit block length of D. For $X \in \{0,1\}^j$, let $|X| \coloneqq j$. The concatenation of two bit strings X and Y is written as $X\|Y$ or XY when no confusion is possible. For integers $0 \leq j \leq i$ and $X \in \{0,1\}^i$, let $\mathsf{msb}_j(X)$ (resp. $\mathsf{lsb}_j(X)$) be the most (resp. least) significant j bits of X. For a non-empty set $\mathcal{S}$, $S \xleftarrow{\$} \mathcal{S}$ means that an element is chosen uniformly at random from $\mathcal{S}$ and assigned to S. For two sets $\mathcal{S}$ and $\mathcal{S}'$, $\mathcal{S} \xleftarrow{\cup} \mathcal{S}'$ means $\mathcal{S} \leftarrow \mathcal{S} \cup \mathcal{S}'$. For an integer $l \geq 0$ and $X \in \{0,1\}^*$, $X_1, \ldots, X_\ell \xleftarrow{l} X$ means parsing of X into fixed-length l-bit strings, where if $X \neq \varepsilon$ then $X = X_1\| \cdots \|X_\ell$, $|X_i| = l$ for $i \in [\ell - 1]$, and $0 < |X_\ell| \leq l$; if $X = \varepsilon$ then $\ell = 1$ and $X_1 = \varepsilon$. For integers $m, n \geq 0$, let $\mathsf{Func}(m,n)$ be the set of all functions from $\{0,1\}^m$ to $\{0,1\}^n$. For an integer $n \geq 0$, let $\mathsf{Perm}(n)$ be the set of all n-bit permutations. For a set $\mathcal{S}$ and $j \in [l]$, let $(y_1, \ldots, y_{j-1}, *, y_{j+1}, \ldots, y_l) \in \mathcal{S}$ be a condition that $\exists y$ s.t. $(y_1, \ldots, y_{j-1}, y, y_{j+1}, \ldots, y_l) \in \mathcal{S}$.

Algorithm 1 CTR

Encryption/Decryption $\mathsf{CTR}[E_K](N, D)$

1: $m \leftarrow |D|_n$; **for** $i = 1, \ldots, m$ **do** $X_{2,i} \leftarrow \mathsf{add}(N, i)$; $Y_{2,i} \leftarrow E_K(X_{2,i})$ **end for**
2: $KS \leftarrow \mathsf{msb}_{|D|}(Y_{2,1} \| \cdots \| Y_{2,m})$; $D' \leftarrow D \oplus KS$; **return** D'

Algorithm 2 CBC

MAC $\mathsf{CBC}[E_K](B)$

1: $b \leftarrow |B|_n$; $B_1, \ldots, B_b \xleftarrow{n} B$; $Y_{1,0} \leftarrow 0^n$
2: **for** $i = 1, \ldots, b$ **do** $X_{1,i} \leftarrow B_i \oplus Y_{1,i-1}$; $Y_{1,i} \leftarrow E_K(X_{1,i})$ **end for**
3: **return** $Y_{1,b}$

Algorithm 3 CCM

Encryption $\mathsf{CCM.Enc}[E_K](N, A, M)$

1: $B \leftarrow \mathsf{f}_{\mathsf{CCM}}(N, A, M)$; $S \leftarrow \mathsf{CBC}[E_K](B)$; $X_{2,0} \leftarrow \mathsf{add}(N, 0)$; $Y_{2,0} \leftarrow E_K(X_{2,0})$
2: $T \leftarrow \mathsf{lsb}_t(S \oplus Y_{2,0})$; $C \leftarrow \mathsf{CTR}[E_K](N, M)$; **return** (C, T)

Decryption $\mathsf{CCM.Dec}[E_K](N, A, C, \widetilde{T})$

1: $M \leftarrow \mathsf{CTR}[E_K](N, C)$; $B \leftarrow \mathsf{f}_{\mathsf{CCM}}(N, A, M)$; $S \leftarrow \mathsf{CBC}[E_K](B)$
2: $X_{2,0} \leftarrow \mathsf{add}(N, 0)$; $Y_{2,0} \leftarrow E_K(X_{2,0})$; $T \leftarrow \mathsf{lsb}_t(S \oplus Y_{2,0})$
3: **if** $T = \widetilde{T}$ **then return** M **else return reject end if**

3 Specification of CCM

CCM is a block-cipher(BC)-based and nonce-based AE scheme with the Encrypt-and-MAC structure. The encryption part is the CTR mode and the MAC part is CBC-MAC, which is simply denoted by CBC throughout the paper.

3.1 Block Cipher (BC)

A BC is a set of permutations indexed by a key. For positive integers k and n, let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be an encryption of a BC with k-bit keys and n-bit blocks. Let $E^{-1} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be its decryption. Let $E^{\pm} := (E, E^{-1})$. E with a key K is denoted by E_K or $E(K, \cdot)$. Similarly, E^{-1} with a key K is denoted by E_K^{-1} or $E^{-1}(K, \cdot)$.

3.2 CTR Mode

CTR is a parallelizable encryption scheme with a BC E_K. The specification of CTR is given in Algorithm 1 and Fig. 2(right). Let c be a parameter for the counters. $\mathsf{CTR}[E_K] : \{0,1\}^\nu \times \{0,1\}^{\leq n(2^c-2)} \to \{0,1\}^{\leq n(2^c-2)}$ takes a tuple of a key K, a nonce N, and a plaintext/ciphertext D, and returns its ciphertext/plaintext D' such that $|D| = |D'|$. If D is a plaintext (resp. ciphertext), then D' is the ciphertext (resp. plaintext). KS is a key stream with which a ciphertext (resp. plaintext) is defined by XORing a plaintext (resp. ciphertext). $\mathsf{add} : \{0,1\}^\nu \times [0, 2^c] \to \{0,1\}^n$ is a function that on an input pair of a nonce

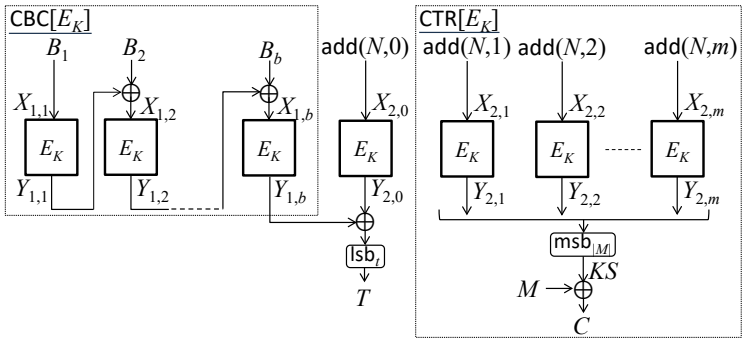

Fig. 2. The encryption of CCM, where $B \leftarrow \mathsf{f}_{\mathsf{CCM}}(N, A, M)$ and $B_1, \ldots, B_b \xleftarrow{n} B$.

and a counter, returns an input block of E such that for any $N \in \{0,1\}^\nu$ and distinct values $i, j \in [0, 2^c]$, $\mathsf{add}(N, i) \neq \mathsf{add}(N, j)$. Note that "$2^c$" is reserved for the first block of CBC and "0" is reserved for masking CBC outputs.

3.3 CBC Mode

CBC is a BC-based MAC that is an iterated construction of E_K. $\mathsf{CBC}[E_K] : \{0,1\}^{n*} \to \{0,1\}^n$ takes a message B of length multiple of n, and returns an n-bit tag $Y_{1,b}$. The specification of CBC is given in Algorithm 2 and Fig. 2(left).

3.4 CCM Mode

CCM is a nonce-based AE scheme with E_K. Let ν be the nonce size such that $\nu \leq n$. Let $\mathcal{M} = \{0,1\}^{\leq n(2^c-2)}$ be plaintext/ciphertext spaces and $\mathcal{A} \subset \{0,1\}^*$ an associated data (AD) space. Let t be the tag size of CCM such that $t \leq n$. The specification of CCM is given in Algorithm 3 and Fig. 2. Let $\mathsf{f}_{\mathsf{CCM}} : \{0,1\}^\nu \times \mathcal{A} \times \mathcal{M} \to \{0,1\}^*$ be an injective formatting function that takes a nonce N, an AD A, and a plaintext M, and returns an encoded message $B = \mathsf{f}_{\mathsf{CCM}}(N, A, M)$ such that its first n-bit block $B_1 = \mathsf{add}(N, 2^c)$, meaning that all first input blocks of CBC are distinct from all input blocks of CTR. The input blocks defined by add, namely $X_{1,1}, X_{2,0}, X_{2,1}, \ldots, X_{2,m}$, are called the nonce-dependent input blocks, and the other input blocks, $X_{1,2}, \ldots, X_{1,b}$, are called the nonce-independent input blocks.

$\mathsf{CCM.Enc}[E_K] : \{0,1\}^\nu \times \mathcal{A} \times \mathcal{M} \to \mathcal{M} \times \{0,1\}^t$ is the encryption of CCM with E_K. It accepts a nonce $N \in \{0,1\}^\nu$, an AD $A \in \mathcal{A}$, and a plaintext $M \in \mathcal{M}$, and returns a ciphertext $C \in \mathcal{M}$ such that $|C| = |M|$.

$\mathsf{CCM.Dec}[E_K] : \{0,1\}^\nu \times \mathcal{A} \times \mathcal{M} \times \{0,1\}^t \to \mathcal{M} \cup \{\mathbf{reject}\}$ is the decryption of CCM with E_K. It accepts a nonce $N \in \{0,1\}^\nu$, an AD $A \in \mathcal{A}$, a cipher $C \in \mathcal{M}$, and a tag $\widetilde{T} \in \{0,1\}^t$ and returns, deterministically, either the distinguished invalid symbol $\mathbf{reject} \notin \mathcal{M}$ or a valid plaintext $M \in \mathcal{M}$.

We define a nonce extracting function $\mathsf{ext}_{\mathsf{nonce}} : \{0,1\}^n \to \{0,1\}^\nu$ that takes an n-bit input block $X \in \{0,1\}^n$ and returns a ν-bit value such that for an input block X, if $\exists N \in \{0,1\}^\nu, i \in [0, 2^c]$ s.t. $X = \mathsf{add}(N, i)$, then $\mathsf{ext}_{\mathsf{nonce}}(X) = N$.

4 Security Definitions and Proof Tools

4.1 Distinguishing Advantage

We consider distinguishing-type security notions for BCs and AEs. We thus define the following distinguishing advantage of an adversary $\mathbf{A}$ that has access to either $\mathcal{O}_1$ or $\mathcal{O}_2$ and returns a decision bit. For $i \in [2]$, let $\mathbf{A}^{\mathcal{O}_i} = 1$ be an event that $\mathbf{A}$ with $\mathcal{O}_i$ returns 1. Then, the distinguishing advantage of $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_1,\mathcal{O}_2}(\mathbf{A}) \coloneqq \Pr\left[\mathbf{A}^{\mathcal{O}_1} = 1\right] - \Pr\left[\mathbf{A}^{\mathcal{O}_2} = 1\right].$$

4.2 Security Models for BCs

In the mu-security proofs of CCM, we consider two models for BCs: the standard multi-user-pseudorandom-permutation (mu-PRP) security and the ideal cipher (IC) models.

Standard Model. In this model, the underlying BCs are assumed to be mu-PRP secure, where BC instantiations with independent keys are securely replaced with independent random permutations (RPs). Let u be the number of users. In the mu-PRP game, an adversary interacts with either the real-world oracles $(E_{K_1}, \ldots, E_{K_u})$ or the ideal-world oracles $(P_1, \ldots, P_u)$, where $\forall \omega \in [u] : K_\omega \xleftarrow{\$} \{0,1\}^k$ and RPs are defined as $\forall \omega \in [u] : P_\omega \xleftarrow{\$} \mathsf{Perm}(n)$. At the end of this game, $\mathbf{A}$ returns a decision bit in $\{0,1\}$. The mu-PRP advantage function of $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{muprp}}_{E}(\mathbf{A}) \coloneqq \mathbf{Adv}^{\mathsf{dist}}_{(E_{K_1},\ldots,E_{K_u}),(P_1,\ldots,P_u)}(\mathbf{A}).$$

For all possible adversaries $\mathbf{A}$ that have access to u users, make at most q queries, and run in time τ, the maximum advantage is defined as

$$\mathbf{Adv}^{\mathsf{muprp}}_{E}(u, q, \tau) \coloneqq \max_{\mathbf{A}} \mathbf{Adv}^{\mathsf{muprp}}_{E}(\mathbf{A}).$$

Ideal Cipher (IC) Model. Let $\mathcal{BC}$ be the set of all encryptions of k-bit key and n-bit block BCs. An IC is an ideal BC and defined as $E \xleftarrow{\$} \mathcal{BC}$. In the IC model, all parties including CCM oracles and adversaries obtain IC's outputs by accessing an IC $E^{\pm} = (E, E^{-1})$.

4.3 Security Models for CCM

Multi-user-AE (mu-AE) security is the indistinguishability between the real and ideal worlds. Let u be the number of users. Let $\$_\omega$ be a random-bit oracle of the ω-th user that takes an input tuple (N, A, M) of a nonce, an AD, and a plaintext, and returns a pair of a random ciphertext and a tag defined as $(C, T) \xleftarrow{\$} \{0,1\}^{|\mathsf{CCM.Enc}[E_K](N,A,M)|}$. Let $\perp_\omega$ be a reject oracle that returns **reject** for any query. Let $K_1, \ldots, K_u$ be users' keys defined as $\forall \omega \in [u] : K_\omega \xleftarrow{\$} \{0,1\}^k$. In the this game, an adversary $\mathbf{A}$ has access to either real-world oracles $\mathcal{O}_{\mathsf{real}}$ or ideal-world oracles $\mathcal{O}_{\mathsf{ideal}}$ defined as follows.

$$\begin{aligned}\textbf{Standard} &: \mathcal{O}^{\mathsf{sm}}_{\mathsf{real}} \coloneqq (\mathsf{CCM}[E_{K_\omega}])_{\omega\in[u]};\ \mathcal{O}^{\mathsf{sm}}_{\mathsf{ideal}} \coloneqq (\$_\omega, \perp_\omega)_{\omega\in[u]},\\ \textbf{IC} &: \mathcal{O}^{\mathsf{icm}}_{\mathsf{real}} \coloneqq (\mathsf{CCM}[E_{K_\omega}])_{\omega\in[u]}, E^{\pm});\ \mathcal{O}^{\mathsf{icm}}_{\mathsf{ideal}} \coloneqq ((\$_\omega, \perp_\omega)_{\omega\in[u]}, E^{\pm}).\end{aligned}$$

At the end of this game, $\mathbf{A}$ return a decision bit in $\{0,1\}$. The mu-AE-security advantage functions of $\mathbf{A}$ are defined as

$$\begin{aligned}\textbf{Standard} &: \mathbf{Adv}^{\mathsf{muae,sm}}_{\mathsf{CCM}}(\mathbf{A}) \coloneqq \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}^{\mathsf{sm}}_{\mathsf{real}},\mathcal{O}^{\mathsf{sm}}_{\mathsf{ideal}}}(\mathbf{A}),\\ \textbf{IC} &: \mathbf{Adv}^{\mathsf{muae,icm}}_{\mathsf{CCM}}(\mathbf{A}) \coloneqq \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}^{\mathsf{icm}}_{\mathsf{real}},\mathcal{O}^{\mathsf{icm}}_{\mathsf{ideal}}}(\mathbf{A}).\end{aligned}$$

Queries to each user are called online queries. Queries to encryption oracles $\mathsf{CCM.Enc}[E_{K_\omega}]$ or $\$_\omega$ (resp. decryption oracles $\mathsf{CCM.Dec}[E_{K_\omega}]$ or $\perp_\omega$) are called encryption (resp. decryption) queries. In the IC model, Queries to an IC are called offline queries, and offline queries to E (resp. E^{-1}) are called forward (resp. inverse) queries.

We consider nonce-respecting adversaries where for each user, all nonces in encryption queries are distinct. Moreover, making a repeated or trivial decryption query is forbidden, where the trivial query $(N, A, C, \widetilde{T})$ is such that the query tuple was obtained by some previous encryption query to the same user.

4.4 Adversaries and Its Resources

In our proofs, we consider computationally-bounded and/or computationally-unbounded adversaries. Queries to encryption oracles $\mathsf{CCM.Enc}[E_{K_\omega}]$ or $\$_\omega$ (resp. decryption oracles $\mathsf{CCM.Dec}[E_{K_\omega}]$ or $\perp_\omega$) are called encryption (resp. decryption) queries. Let q_{e} be the number of encryption queries, q_{d} be the number of decryption queries, and σ be the number of BC invocations in online queries. and σ_ω the number of BC invocations in online queries to the ω-th user such that $\sum_{\omega\in[u]} \sigma_\omega = \sigma$. For computationally-bounded (resp. computationally-unbounded) adversaries, the time resources are expressed by its running time τ (resp. the number of offline queries to an IC denoted by p). Let σ_{u} be the maximum number of BC invocations per user, i.e., $\forall \omega \in [u] : \sigma_\omega \le \sigma_{\mathsf{u}}$. Let $\mathcal{A}_{\mathsf{sm}}$ (resp. $\mathcal{A}_{\mathsf{icm}}$) be the set of all possible adversaries in the standard (resp. IC) model with the above resources.

4.5 Definitions for Proofs

In our proofs, we use the following notations and definitions.

- For $\alpha \in [p]$, let $(\hat{K}^{(\alpha)}, \hat{X}^{(\alpha)}, \hat{Y}^{(\alpha)})$ be the α-th offline query-response tuples such that $\hat{Y}^{(\alpha)} = E(\hat{K}^{(\alpha)}, \hat{X}^{(\alpha)})$.
- For $\omega \in [u]$ and $\alpha \in [q]$, ω is called "user index" and α is called "query index."
- For $\alpha \in [q]$, values corresponding with the α-th online query are denoted by using the superscript symbol of (α) such as $M^{(\alpha)}$, $C^{(\alpha)}$, $N^{(\alpha)}$, $A^{(\alpha)}$, etc. The lengths b and m for the α-th online query are denoted by b_α and m_α, respectively. Let $\mathsf{u}_\alpha \in [u]$ be the user index for the α-th online query. If an α-th online query is to an ω-th user, then $\mathsf{u}_\alpha = \omega$.
- Let $\mathcal{Q}_{\mathsf{Enc}} \subseteq [q]$ (resp. $\mathcal{Q}_{\mathsf{Dec}} \subseteq [q]$) be the set of encryption (resp. decryption) query indexes. Let $\mathcal{Q}_{\mathsf{Enc}}^{[\omega]} \subseteq \mathcal{Q}_{\mathsf{Enc}}$ (resp. $\mathcal{Q}_{\mathsf{Dec}}^{[\omega]} \subseteq \mathcal{Q}_{\mathsf{Dec}}$) be the set of encryption (resp. decryption) query indexes of the ω-th user. Let $\mathcal{Q}^{[\omega]} := \mathcal{Q}_{\mathsf{Enc}}^{[\omega]} \cup \mathcal{Q}_{\mathsf{Dec}}^{[\omega]}$ be the set of online query indexes of the ω-th user.
- For $\alpha \in [q]$, let $\mathsf{Index}^{(\alpha)} := (\{1\} \times [b_\alpha]) \cup (\{2\} \times [0, m_\alpha])$ be the set of indexes of input-output pairs in the α-th online query.
- Let $\mathcal{X}^{[\omega]} \coloneqq \{X_{i,j}^{(\alpha)} \mid \alpha \in \mathcal{Q}^{[\omega]}, (i,j) \in \mathsf{Index}^{(\alpha)}\}$ be all input blocks for the ω-th user. Let $\mathcal{X}_{\mathsf{Enc}}^{[\omega]} \coloneqq \{X_{i,j}^{(\alpha)} \mid \alpha \in \mathcal{Q}_{\mathsf{Enc}}^{[\omega]}, (i,j) \in \mathsf{Index}^{(\alpha)}\}$ be all input blocks for encryption queries to the ω-th user. Let $\mathcal{X}_2^{[\omega]} \coloneqq \{(X_{2,j}^{(\gamma)}, Y_{2,j}^{(\gamma)}) \mid \gamma \in \mathcal{Q}^{[\omega]}, j \in [0, m_\gamma]\}$ be all input-output pairs defined in CTR and the tag generation of the ω-th user. Let $\mathcal{X}_{\mathsf{N}}^{[\omega]} \coloneqq \{X_{1,1}^{(\alpha)}, X_{2,1}^{(\alpha)}, \ldots, X_{2,m_\alpha}^{(\alpha)} \mid \alpha \in \mathcal{Q}^{[\omega]}\}$ be the set of nonce-dependent input blocks for the ω-th user. Let $\mathcal{X}_{\neq \mathsf{N}}^{[\omega]} \coloneqq \{X_{1,2}^{(\alpha)}, \ldots, X_{1,b_\alpha}^{(\alpha)} \mid \alpha \in \mathcal{Q}^{[\omega]}\}$ be the set of nonce-independent input blocks for the ω-th user.
- Let $\mathcal{Y}^{[\omega]} \coloneqq \{Y_{i,j}^{(\alpha)} \mid \alpha \in \mathcal{Q}^{[\omega]}, (i,j) \in \mathsf{Index}^{(\alpha)}\}$ be the set of output blocks for the ω-th user.
- We call "a query phase" a phase that an adversary makes queries to its oracles and "a decision phase" a phase after finishing all queries and before outputting a decision bit.

5 Mu-Security of CCM in the Standard Model

We give an mu-bound of CCM in the standard model and the security proof.

5.1 Security Bound

Theorem 1 (Mu-Security of CCM in the Standard Model). $\forall \mathbf{A} \in \mathcal{A}_{\mathsf{sm}}$*:*

$$\mathbf{Adv}_{\mathsf{CCM}}^{\mathsf{muae,sm}}(\mathbf{A}) \leq \mathbf{Adv}_{E}^{\mathsf{muprp}}(u, \sigma, \tau + O(\sigma)) + \left(\sum_{\omega \in [u]} \frac{\sigma_\omega^2}{2^n}\right) + \frac{q_{\mathsf{d}}}{2^t}.$$

With the parameters σ and σ_{u}, $\forall \mathbf{A} \in \mathcal{A}_{\mathsf{sm}}$:

$$\mathbf{Adv}_{\mathsf{CCM}}^{\mathsf{muae,sm}}(\mathbf{A}) \leq \mathbf{Adv}_{E}^{\mathsf{muprp}}(u, \sigma, \tau + O(\sigma)) + \frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t}.$$

5.2 Proof of Theorem 1

Without loss of generality, assume that $\mathbf{A}$ is deterministic. Let σ_ω be the number of BC calls in online queries to the ω-th user, where $\sigma_\omega \le \sigma_{\mathsf{u}}$. In this proof, we consider four games.

Real World $\rightarrow$ Game 2. We start the proof from the real world, followed by Game 2. In the real world, $\mathbf{A}$ has access to $\mathcal{O}_{\mathsf{real}}$. From the real world to Game 2, the u BCs $(E_{K_\omega})_{\omega\in[u]}$ are replaced with u RPs $(P_\omega)_{\omega\in[u]}$, where $\forall\omega \in [u] : P_\omega \xleftarrow{\$} \mathsf{Perm}(n)$. Hence, in Game 2, $\mathbf{A}$ has access to the modified oracles $\mathcal{O}_2 := (\mathsf{CCM}[P_\omega])_{\omega\in[u]}$. The BC-RP switch yields the following bound.

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_{\mathsf{real}},\mathcal{O}_2}(\mathbf{A}) \le \mathbf{Adv}^{\mathsf{muprp}}_{E}(\sigma,\tau+O(\sigma)).$$

Game 2 $\rightarrow$ Game 3. We next consider Game 3. Hereafter, we consider a computationally-unbounded adversary $\mathbf{A}$. From Game 2 to Game 3, the RPs $(P_\omega)_{\omega\in[u]}$ are replaced with random functions (RFs) $(\mathcal{R}_\omega)_{\omega\in[u]}$, where $\forall\omega \in [u] : \mathcal{R}_\omega \xleftarrow{\$} \mathsf{Func}(n,n)$. Hence, in Game 3, $\mathbf{A}$ has access to the modified oracles $\mathcal{O}_3 := (\mathsf{CCM}[\mathcal{R}_\omega])_{\omega\in[u]}$. For each $\omega \in [u]$, a RF $\mathcal{R}_\omega$ is the same as a RP as long as no output collision occurs, and the collision probability is $\binom{\sigma_\omega}{2}\cdot\frac{1}{2^n} \le \frac{0.5\sigma_\omega^2}{2^n}$. Hence, by the RP-RF switch, we have

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_2,\mathcal{O}_3}(\mathbf{A}) \le \sum_{\omega\in[u]}\frac{0.5\sigma_\omega}{2^n}.$$

Game 3 $\rightarrow$ Ideal World. Finally, we evaluate the difference between Game 3 and the ideal world. We derive the following bound.

Lemma 1. *For any computationally-unbounded adversary* $\mathbf{A}$*,*

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_3,\mathcal{O}_{\mathsf{ideal}}}(\mathbf{A}) \le \frac{q_{\mathsf{d}}}{2^t} + \sum_{\omega\in[u]}\frac{0.5\sigma_\omega^2}{2^n},$$

where $\mathcal{O}_3 = (\mathsf{CCM}[\mathcal{R}_\omega])_{\omega\in[u]}$ *and* $\mathcal{O}_{\mathsf{ideal}} = (\$_\omega,\perp_\omega)_{\omega\in[u]}$.

Hereafter, we provide a high-level overview of the proof of Lemma 1, and the formal proof is given in the full version of this paper [22].

Proof of Lemma 1 (Overview). We first consider encryption queries in Game 3. For each user, all input blocks $X^{(\alpha)}_{2,i}$ in CTR are distinct, and the outputs $Y^{(\alpha)}_{2,i}$ are chosen independently and uniformly at random from $\{0,1\}^n$. Hence, the responses $(C^{(\alpha)},T^{(\alpha)})$ to the encryption queries are indistinguishable from those defined by $\$_\omega$ in the ideal world.

The remaining work is to evaluate the difference of responses to decryption queries between Game 3 and the ideal world. In Game 3, for some response of

the decryption query, a valid plaintext ($\neq$ **reject**) is probabilistically returned, and we have

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_3,\mathcal{O}_{\mathsf{ideal}}}(\mathbf{A}) \leq \Pr[\exists \beta \in \mathcal{Q}_{\mathsf{Dec}} \text{ s.t. } T^{(\beta)} = \widetilde{T}^{(\beta)}].$$

We evaluate the probability by using the following event:

$$\mathsf{coll}_{X_{1,b}} \Leftrightarrow \exists \beta \in \mathcal{Q}_{\mathsf{Dec}} \text{ s.t. } X^{(\beta)}_{1,b_\beta} \in \mathcal{X}^{[\mathsf{u}_\beta]}_{\mathsf{Enc}}.$$

The event means that for some decryption query, the last input block in CBC collides with some input block defined by the encryption query. In other worlds, if the event does not occur, then all tags $T^{(\beta)}$ are defined independently of the responses of the encryption queries. Thus,

$$\Pr[\exists \beta \in \mathcal{Q}_{\mathsf{Dec}} \text{ s.t. } T^{(\beta)} = \widetilde{T}^{(\beta)} \mid \neg\mathsf{coll}_{X_{1,b}}] \leq \frac{q_{\mathsf{d}}}{2^t},$$

and

$$\begin{aligned}\mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_3,\mathcal{O}_{\mathsf{ideal}}}(\mathbf{A}) &\leq \Pr[\exists \beta \in \mathcal{Q}_{\mathsf{Dec}} \text{ s.t. } T^{(\beta)} = \widetilde{T}^{(\beta)} \mid \neg\mathsf{coll}_{X_{1,b}}] + \Pr[\mathsf{coll}_{X_{1,b}}] \\ &\leq \frac{q_{\mathsf{d}}}{2^t} + \Pr[\mathsf{coll}_{X_{1,b}}].\end{aligned}$$

We evaluate the probability $\Pr[\mathsf{coll}_{X_{1,b}}]$. By the iterated structure of CBC and the property of add,[9] the event $\mathsf{coll}_{X_{1,b}}$ implies that there exists $\beta \in \mathcal{Q}_{\mathsf{Dec}}$, and $j \in [b_\beta]$ such that the j-th CBC input block is $X^{(\beta)}_{1,j} \in \mathcal{X}^{[\mathsf{u}_\beta]}_{\mathsf{Enc}}$ but the previous input block is $X^{(\beta)}_{1,j-1} \notin \mathcal{X}^{[\mathsf{u}_\beta]}_{\mathsf{Enc}}$. The j-th input block has the form of $X^{(\beta)}_{1,j} = B^{(\beta)}_j \oplus Y^{(\beta)}_{1,j-1}$ and $Y^{(\beta)}_{1,j-1}$ is chosen independently of all output blocks for the encryption queries. Using the randomness of $Y^{(\beta)}_{1,j-1}$, we have the following birthday bound:

$$\Pr[\mathsf{coll}_{X_{1,b}}] \leq \sum_{\omega \in [u]} \binom{\sigma_\omega}{2} \cdot \frac{1}{2^n} \leq \sum_{\omega \in [u]} \frac{0.5\sigma^2_\omega}{2^n}.$$

By using the above bounds, we obtain the bound in Lemma 1.

■ (Lemma 1 (Overview))

Conclusion of the Proof. By using these bounds, we have

$$\begin{aligned}\mathbf{Adv}^{\mathsf{muae,sm}}_{\mathsf{CCM}}(\mathbf{A}) &\leq \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_{\mathsf{real}},\mathcal{O}_2}(\mathbf{A}) + \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_2,\mathcal{O}_3}(\mathbf{A}) + \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_3,\mathcal{O}_{\mathsf{ideal}}}(\mathbf{A}) \\ &\leq \mathbf{Adv}^{\mathsf{muprp}}_{E}(u, \sigma, \tau + O(\sigma)) + \sum_{\omega \in [u]} \frac{0.5\sigma^2_\omega}{2^n} + \frac{q_{\mathsf{d}}}{2^t}.\end{aligned}$$

■ (Theorem 1)

[9] The property of add ensures that for each $\omega \in [u]$, $\alpha \in \mathcal{Q}^{[\omega]}_{\mathsf{Enc}}$, and $\beta \in \mathcal{Q}^{[\omega]}_{\mathsf{Dec}}$, the messages $B^{(\alpha)}$ and $B^{(\beta)}$ of CBC are distinct and the first input block $B^{(\beta)}_1$ is distinct from all input blocks in CTR, offering the condition $\exists \beta, j$ s.t. $(X^{(\beta)}_{1,j-1} \notin \mathcal{X}^{[\mathsf{u}_\beta]}_{\mathsf{Enc}}) \wedge (X^{(\beta)}_{1,j} \in \mathcal{X}^{[\mathsf{u}_\beta]}_{\mathsf{Enc}})$.

6 Mu-Security of CCM with NR

We evaluate the security of CCM with randomized nonce in the IC model. We use the d-bound model by Hoang and Tessaro [13], which is a generalization of the randomized nonce.

6.1 d-bound Adversaries

In the d-bound model, the number of collisions of nonces in encryption queries across users is bounded by d. Note that there is no collision in nonces in encryption queries within the same user.

Definition 1 (d-bound model). *For $\omega \in [u]$, let $\mathcal{N}^{[\omega]}$ be the set of nonces in encryption queries to the ω-th user. A d-bound adversary is such that for any $N \in \{0,1\}^\nu$, $|\{\omega \in [u] \mid N \in \mathcal{N}^{[\omega]}\}| \le d$.*

The parameter d can be small by using a random nonce: each original nonce N_{orig} is defined by incrementing 1, i.e., $N_{\mathrm{orig}} \leftarrow N_{\mathrm{orig}} + 1$ (initially $N_{\mathrm{orig}} = 0^n$), and a randomized nonce N is defined as $N = N_{\mathrm{orig}} \oplus R$ with the ν-bit original nonce N_{orig} and a user-specific random mask $R \in \{0,1\}^\nu$.

We study the bound d. We consider the following randomized nonce: each original nonce N_{orig} is defined by incrementing 1, i.e., $N_{\mathrm{orig}} \leftarrow N_{\mathrm{orig}} + 1$ (initially $N_{\mathrm{orig}} = 0^n$), and a randomized nonce N is defined as $N = N_{\mathrm{orig}} \oplus R$ with the ν-bit original nonce N_{orig} and a user-specific random mask $R \in \{0,1\}^\nu$. Then, for each of d randomized nonces $N^{(\alpha_1)}, \ldots, N^{(\alpha_d)}$ such that the user indexes $\mathsf{u}_{\alpha_1}, \ldots, \mathsf{u}_{\alpha_d}$ are all distinct, we have $\Pr[N^{(\alpha_1)} = \ldots = N^{(\alpha_d)}] \le \left(\frac{1}{2^\nu}\right)^{d-1}$. Using the bound with $d := \frac{\nu}{\log_2 \nu}$, we have

$$\begin{aligned}
\Pr[\exists \alpha_1, \ldots, \alpha_d \text{ s.t. } N^{(\alpha_1)} = \ldots = N^{(\alpha_d)}] &\le \binom{q_{\mathsf{e}}}{d} \cdot \left(\frac{1}{2^\nu}\right)^{d-1} \\
&\le 2^\nu \left(\frac{e q_{\mathsf{e}}}{d 2^\nu}\right)^d = 2^\nu \left(\frac{e q_{\mathsf{e}}}{\frac{\nu}{\log_2 \nu} \cdot 2^\nu}\right)^{\frac{\nu}{\log_2 \nu}} \\
&\le \left((2^\nu)^{\frac{\log_2 \nu}{\nu}} \cdot \frac{e q_{\mathsf{e}}}{\frac{\nu}{\log_2 \nu} \cdot 2^\nu}\right)^{\frac{\nu}{\log_2 \nu}} \\
&\le \left(\frac{3(\log_2 \nu) q_{\mathsf{e}}}{2^\nu}\right)^{\frac{\nu}{\log_2 \nu}},
\end{aligned}$$

using Stirling's approximation ($d! \ge (d/e)^d$ for any d). We then consider for the common parameter for CCM: the nonce size is $\nu = 3n/4$ ($\nu = 96$ when using the AES parameter $n = 128$). In this case, $d = \frac{3n/4}{\log_2(3n/4)}$ and the bound of d can be ensured up to $q_{\mathsf{e}} \approx 2^{3n/4}$ encryption queries.

6.2 Security Bound

The mu-security bound of CCM with NR is given below.

Theorem 2 (Mu-Security of CCM with NR in the IC Model). $\forall \mathbf{A} \in \mathcal{A}_{\mathsf{icm}}$ *such that* $\mathbf{A}$ *is a d-bound adversary:*

$$\mathbf{Adv}^{\mathsf{muae,icm}}_{\mathsf{CCM}}(\mathbf{A}) \leq \frac{q_{\mathsf{d}}}{2^t} + \sum_{\omega \in [u]} \frac{\sigma_\omega^2}{2^n} + \frac{\left(d + \frac{n}{\log_2 n}\right)(p+\sigma)}{2^k} + \left(\frac{3(\log_2 n)\sigma}{2^n}\right)^{\frac{n}{\log_2 n}} + \frac{\sigma(p+\sigma)}{2^{k+n}}.$$

With the parameters σ *and* σ_{u}, $\forall \mathbf{A} \in \mathcal{A}_{\mathsf{icm}}$ *such that* $\mathbf{A}$ *is a d-bound adversary:*

$$\mathbf{Adv}^{\mathsf{muae,icm}}_{\mathsf{CCM}}(\mathbf{A}) \leq \frac{q_{\mathsf{d}}}{2^t} + \frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{\left(d + \frac{n}{\log_2 n}\right)(p+\sigma)}{2^k} + \left(\frac{3(\log_2 n)\sigma}{2^n}\right)^{\frac{n}{\log_2 n}} + \frac{\sigma(p+\sigma)}{2^{k+n}}.$$

Assume that $n \leq k$. The last three terms excluding p are of online security and become a constant if σ is about 2^n. On the other hand, the second term becomes a constant if σ is about $\frac{2^n}{\sigma_u}$. Hence, the first two terms are dominant online terms. The last term excluding σ is of offline security and becomes a constant if $p = \frac{2^{k+n}}{\sigma}$. Since $\sigma \leq 2^n$, the third term excluding σ is a dominant offline term. Since d is about $\frac{n}{\log_2 n}$, dominant terms in the bound is $\frac{q_{\mathsf{d}}}{2^t} + \frac{\sigma_{\mathsf{u}}\sigma}{2^n} + \frac{dp}{2^k}$.

6.3 Proof of Theorem 2

Without loss of generality, we assume that $\mathbf{A}$ is deterministic. In this evaluation, we consider three games.

Real World → Game 2. We start the proof from the real world, followed by Game 2. In the real world, $\mathbf{A}$ has access to $\mathcal{O}_{\mathsf{real}}$. From the real world to Game 2, the u BCs $(E_{K_\omega})_{\omega \in [u]}$ are replaced with u RFs $(\mathcal{R}_\omega)_{\omega \in [u]}$. Hence, in Game 2, $\mathbf{A}$ has access to the modified oracles $\mathcal{O}_2 \coloneqq ((\mathsf{CCM}[\mathcal{R}_\omega])_{\omega \in [u]}, E^{\pm})$, where $E \xleftarrow{\$} \mathcal{BC}$ and $\forall \omega \in [u] : \mathcal{R}_\omega \xleftarrow{\$} \mathsf{Func}(n,n)$. The following lemma shows an upper-bound of the difference between the real world and Game 2.

Lemma 2. *For any computationally-unbounded adversary* $\mathbf{A}$*,*

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_{\mathsf{real}},\mathcal{O}_2}(\mathbf{A}) \leq \frac{\left(d + \frac{n}{\log_2 n}\right)(p+\sigma)}{2^k} + \frac{\sigma(p+\sigma)}{2^{k+n}} + \left(\frac{3(\log_2 n)\sigma}{2^n}\right)^{\frac{n}{\log_2 n}} + \sum_{\omega \in [u]} \frac{0.5\sigma_\omega^2}{2^n},$$

where $\mathcal{O}_{\mathsf{real}} = ((\mathsf{CCM}[E_{K_\omega}])_{\omega \in [u]}, E^{\pm})$ *and* $\mathcal{O}_2 = ((\mathsf{CCM}[\mathcal{R}_\omega])_{\omega \in [u]}, E^{\pm})$.

Hereafter, we provide a high-level overview of the proof, and the formal proof is given in the full version of this paper [22].

Proof of Lemma 2 (Overview). From the real world to Game 2, the underlying primitives are replaced from an IC E (with independent keys) to independent RFs $(\mathcal{R}_\omega)_{\omega\in[u]}$. We thus define the following three events that are taken into account the difference.

EVENT $\mathsf{coll}_{\mathsf{on},\neq\mathsf{u}}$. We first define the following event:

$$\mathsf{coll}_{\mathsf{on},\neq\mathsf{u}} \Leftrightarrow \exists\omega_1,\omega_2\in[u] \text{ s.t. } \omega_1\neq\omega_2 \wedge K^{[\omega_1]}=K^{[\omega_2]} \\ \wedge (\mathcal{X}^{[\omega_1]}\cap\mathcal{X}^{[\omega_2]}\neq\emptyset \vee \mathcal{Y}^{[\omega_1]}\cap\mathcal{Y}^{[\omega_2]}\neq\emptyset),$$

which considers a collision of pairs of key and input/output block between distinct users. If it does not occur in the real world, for each user, the underlying primitive can be independent of those of the other users as Game 2. $\mathcal{X}^{[\omega_1]}\cap\mathcal{X}^{[\omega_2]}\neq\emptyset$ is the condition on the input-block collision and $\mathcal{Y}^{[\omega_1]}\cap\mathcal{Y}^{[\omega_2]}\neq\emptyset$ is the one on the output-block collision.

We consider the collisions $K^{[\omega_1]}=K^{[\omega_2]}\wedge\mathcal{X}^{[\omega_1]}\cap\mathcal{X}^{[\omega_2]}\neq\emptyset$.

– If $\mathcal{X}_{\mathsf{N}}^{[\omega_1]}\cap\mathcal{X}_{\mathsf{N}}^{[\omega_2]}\neq\emptyset$, i.e., a collision occurs in nonce-dependent input blocks, then a collision of nonces between distinct users occurs. In the d-bound model, for each nonce $N^{(\alpha)}$ of the ω_1-th user, the number of the other different users with the same nonce is at most d. Hence, for each pair of key and nonce, the probability that the pair collides with one of the pairs of the other different users is at most $\frac{d}{2^k}$. Thus, we have

$$\Pr[K^{[\omega_1]}=K^{[\omega_2]}\wedge\mathcal{X}_{\mathsf{N}}^{[\omega_1]}\cap\mathcal{X}_{\mathsf{N}}^{[\omega_2]}\neq\emptyset]\leq\sum_{\alpha\in[q]}\frac{d}{2^k}=\frac{dq}{2^k}.$$

– If $\mathcal{X}_{\neq\mathsf{N}}^{[\omega_1]}\cap\mathcal{X}^{[\omega_2]}\neq\emptyset$, i.e., a collision with nonce-independent input blocks occurs, then each input block $X_{1,j}^{(\alpha)}\in\mathcal{X}_{\neq\mathsf{N}}^{[\omega_1]}$ is defined as $X_{1,j}^{(\alpha)}=B_{1,j}^{(\alpha)}\oplus Y_{1,j-1}^{(\alpha)}$ where $Y_{1,j-1}^{(\alpha)}$ is an n-bit random value. Hence, we can use the n-bit randomness, providing the bound

$$\Pr[K^{[\omega_1]}=K^{[\omega_2]}\wedge\mathcal{X}_{\neq\mathsf{N}}^{[\omega_1]}\cap\mathcal{X}^{[\omega_2]}\neq\emptyset]\leq\binom{\sigma}{2}\cdot\frac{1}{2^{k+n}}\leq\frac{\sigma^2}{2^{k+n}}.$$

We next consider the collisions $K^{[\omega_1]}=K^{[\omega_2]}\wedge\mathcal{Y}^{[\omega_1]}\cap\mathcal{Y}^{[\omega_2]}\neq\emptyset$. The evaluation is the same as the one for the collisions $K^{[\omega_1]}=K^{[\omega_2]}\wedge\mathcal{X}_{\mathsf{N}}^{[\omega_1]}\cap\mathcal{X}_{\mathsf{N}}^{[\omega_2]}\neq\emptyset$. In this case, instead of the multi-collision bound d for input blocks, we use a multi-collision event for output blocks $\cup_{\omega\in[u]}\mathcal{Y}^{[\omega]}$. By using the randomness of the output blocks, the probability that $(\frac{n}{\log_2 n})$-multi-collision occurs in the output blocks can be bounded by $(\frac{3(\log_2 n)\sigma}{2^n})^{\frac{n}{\log_2 n}}$. Assuming that the multi-collision

does not occur, by the same evaluation (but d is replaced with the bound $\frac{n}{\log_2 n}$), we have

$$\Pr[K^{[\omega_1]} = K^{[\omega_2]} \wedge \mathcal{Y}^{[\omega_1]} \cap \mathcal{Y}^{[\omega_2]} \neq \emptyset] \leq \frac{\frac{n}{\log_2 n} \cdot \sigma}{2^k}.$$

Summing these bounds, we have the following bound:

$$\Pr[\mathsf{coll}_{\mathsf{on},\neq\mathsf{u}}] \leq \frac{\left(d + \frac{n}{\log_2 n}\right)\sigma}{2^k} + \left(\frac{3(\log_2 n)\sigma}{2^n}\right)^{\frac{n}{\log_2 n}} + \frac{\sigma^2}{2^{k+n}}.$$

Event $\mathsf{coll}_{\mathsf{on},\mathsf{off}}$. In Game 2, the underlying primitives $(\mathcal{R}_\omega)_{\omega\in[u]}$ are independent of $E^{\pm}$. On the other hand, in the real world, all underlying primitives are E (with independent keys). We thus define the following event for the difference:

$$\begin{aligned}\mathsf{coll}_{\mathsf{on},\mathsf{off}} \Leftrightarrow \alpha \in [q], (i,j) \in \mathsf{Index}^{(\alpha)}, \beta \in [p] \text{ s.t.} \\ K^{[\mathsf{u}_\alpha]} = \hat{K}^{(\beta)} \wedge (X_{i,j}^{(\alpha)} = \hat{X}^{(\beta)} \vee Y_{i,j}^{(\alpha)} = \hat{Y}^{(\beta)}).\end{aligned}$$

The event considers a collision of pairs of key and input/output block between online and offline queries. If it does not occur, outputs of user's primitives can be independent of offline query-response tuples. The evaluation is similar to the evaluation for the event $\mathsf{coll}_{\mathsf{on},\neq\mathsf{u}}$. By using the d-bound model for the input-block collision and the $(\frac{n}{\log_2 n})$-multi-collision event for the output-block collision, we can obtain

$$\Pr[\mathsf{coll}_{\mathsf{on},\mathsf{off}}] \leq \frac{\left(d + \frac{n}{\log_2 n}\right)p}{2^k} + \frac{\sigma p}{2^{k+n}}.$$

Event $\mathsf{coll}_{\mathsf{on},=\mathsf{u}}$. In Game 2, for each $\omega \in [u]$, each output of the underlying primitive $\mathcal{R}_\omega$ is chosen with replacement. On the other hand, in the real world, all underlying primitives are E (with independent keys) and for each $\omega \in [u]$, each output of the underlying primitive is chosen without replacement. We thus define the following event for the RP-RF difference:

$$\begin{aligned}\mathsf{coll}_{\mathsf{on},=\mathsf{u}} \Leftrightarrow \exists \omega \in [u], X_{i_1,j_1}^{(\alpha_1)}, X_{i_2,j_2}^{(\alpha_2)} \in \mathcal{X}^{[\omega]} \text{ s.t.} \\ X_{i_1,j_1}^{(\alpha_1)} \neq X_{i_2,j_2}^{(\alpha_2)} \wedge Y_{i_1,j_1}^{(\alpha_1)} = Y_{i_2,j_2}^{(\alpha_2)},\end{aligned}$$

where $Y_{i_1,j_1}^{(\alpha_1)}$ and $Y_{i_2,j_2}^{(\alpha_2)}$ are independently chosen. By the birthday analysis, we have

$$\Pr[\mathsf{coll}_{\mathsf{on},=\mathsf{u}}] \leq \sum_{\omega\in[u]} \binom{\sigma_\omega}{2} \cdot \frac{1}{2^n} \leq \sum_{\omega\in[u]} \frac{0.5\sigma_\omega^2}{2^n}.$$

Deriving the Bound in Lemma 2. These events cover the differences from the replacements of the underlying primitives from $(E_{K_\omega})_{\omega\in[u]}$ to $(\mathcal{R}_\omega)_{\omega\in[u]}$, thus

by the above bounds,

$$\begin{aligned}\mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_{\mathsf{real}},\mathcal{O}_2}(\mathbf{A}) &\le \Pr[\mathsf{coll}_{\mathsf{on},\neq\mathsf{u}}] + \Pr[\mathsf{coll}_{\mathsf{on},\mathsf{off}}] + \Pr[\mathsf{coll}_{\mathsf{on},=\mathsf{u}}] \\ &\le \frac{\left(d + \frac{n}{\log_2 n}\right)(p+\sigma)}{2^k} + \frac{\sigma(p+\sigma)}{2^{k+n}} \\ &\quad + \left(\frac{3(\log_2 n)\sigma}{2^n}\right)^{\frac{n}{\log_2 n}} + \sum_{\omega\in[u]} \frac{0.5\sigma_\omega^2}{2^n}.\end{aligned}$$

■ (Lemma 2 (Overview))

Game 2 → Ideal World. For the difference between Game 2 and the ideal world, we use Lemma 1 in the proof of Theorem 1. In Lemma 1, an IC is absent, whereas in this evaluation, an IC is available. However, the responses of online queries are independent of the IC, thus an adversary can simulate an IC. Hence, the difference between Game 2 and the ideal world can be bounded by the bound in Lemma 1, and we have

$$\mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_2,\mathcal{O}_{\mathsf{ideal}}}(\mathbf{A}) \le \left(\sum_{\omega\in[u]} \frac{0.5\sigma_\omega^2}{2^n}\right) + \frac{q_{\mathsf{d}}}{2^t}.$$

Conclusion of the Proof. Using the above bounds, we have

$$\begin{aligned}\mathbf{Adv}^{\mathsf{muae},\mathsf{icm}}_{\mathsf{CCM}}(\mathbf{A}) &\le \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_{\mathsf{real}},\mathcal{O}_2}(\mathbf{A}) + \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_2,\mathcal{O}_{\mathsf{ideal}}}(\mathbf{A}) \\ &\le \frac{q_{\mathsf{d}}}{2^t} + \sum_{\omega\in[u]} \frac{\sigma_\omega^2}{2^n} + \frac{\left(d + \frac{n}{\log_2 n}\right)(p+\sigma)}{2^k} \\ &\quad + \left(\frac{3(\log_2 n)\sigma}{2^n}\right)^{\frac{n}{\log_2 n}} + \frac{\sigma(p+\sigma)}{2^{k+n}}.\end{aligned}$$

■ (Theorem 2)

7 Mu-Security of CCM with NKD

In this section, we consider the mu-security of CCM_NKD, CCM with the nonce-based key derivation NKD, following the previous application to GCM [11]. Compared to CCM with NR, CCM_NKD replaces the dominant term $\frac{\sigma_{\mathsf{u}}\sigma}{2^n}$ to $\frac{\sigma_{\mathsf{n}}\sigma}{2^n}$, wherein σ_{n} is the maximum number of BC invocations within the same nonce and user's key, thus its online security becomes independent of σ_{u}.

7.1 Specification of CCM_NKD

Let $\mathsf{F}_K : \{0,1\}^\nu \to \{0,1\}^k$ be a KDF with a κ-bit key K that accepts a nonce and returns a nonce-based key of CCM. The encryption and decryption algorithms of CCM_NKD are defined in the following.

– For an input tuple $(N, A, M) \in \{0,1\}^\nu \times \mathcal{A} \times \mathcal{M}$, the encryption is defined as

$$\mathsf{CCM\_NKD.Enc}[E, \mathsf{F}_K](N, A, M) \coloneqq \mathsf{CCM.Enc}[E_{\mathsf{F}_K(N)}](N, A, M).$$

– For an input tuple $(N, A, C, \widetilde{T}) \in \{0,1\}^\nu \times \mathcal{A} \times \mathcal{M} \times \{0,1\}^t$, the decryption is defined as

$$\mathsf{CCM\_NKD.Dec}[E, \mathsf{F}_K](N, A, C, \widetilde{T}) \coloneqq \mathsf{CCM.Dec}[E_{\mathsf{F}_K(N)}](N, A, C, \widetilde{T}).$$

7.2 Multi-user PRF Security

In our proof, we assume that the KDF is mu-pseudorandom function (mu-PRF) secure. Let u be the number of users. In the mu-PRF-security game, an adversary $\mathbf{A}$ has access to either real-world oracles $(\mathsf{F}_{K_1}, \ldots, \mathsf{F}_{K_u})$ or ideal-world ones $(\mathcal{R}_1, \ldots, \mathcal{R}_u)$, where K_i is the i-th user's key defined as $K_i \xleftarrow{\$} \{0,1\}^\kappa$ and $\mathcal{R}_i$ is a random function of the i-th user defined as $\mathcal{R}_i \xleftarrow{\$} \mathsf{Func}(\nu, k)$. At the end of this game, $\mathbf{A}$ return a decision bit. Then, the mu-PRF-security advantage function of $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}(\mathbf{A}) \coloneqq \mathbf{Adv}^{\mathsf{dist}}_{(\mathsf{F}_{K_\omega})_{\omega\in[u]},(\mathcal{R}_\omega)_{\omega\in[u]}}(\mathbf{A}).$$

For all possible adversaries $\mathbf{A}$ that have access to u users, make at most q queries, and run in time τ, the maximum advantage is defined as

$$\mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}(u, q, \tau) \coloneqq \max_{\mathbf{A}} \mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}(\mathbf{A}).$$

7.3 Mu-Security of CCM_NKD

For each nonce, the KDF in CCM_NKD provides a fresh key of CCM under the assumption that F_K is a secure PRF. Hence, in the mu-setting, there are at most q keys of CCM via the KDF in CCM_NKD. By using the bounds in Theorems 1 and 2, we obtain the following bounds of the mu-AE security of CCM_NKD. Let σ_{n} be the maximum number of BC invocations whose keys are defined by CCM_NKD with the same nonce and user's key.

Corollary 1 (Mu-Security of CCM_NKD in the Standard Model). *For any computationally-bounded adversary* $\mathbf{A}$,

$$\mathbf{Adv}^{\mathsf{muae,sm}}_{\mathsf{CCM\_NKD}}(\mathbf{A}) \le \frac{\sigma_{\mathsf{n}}\sigma}{2^n} + \frac{q_{\mathsf{d}}}{2^t} + \mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}(u, q, \tau + O(\sigma)) + \mathbf{Adv}^{\mathsf{muprp}}_{E}(q, \sigma, \tau + O(\sigma)).$$

Corollary 2 (Mu-Security of CCM_NKD in the d-bound and IC Models). *For any computationally-bounded adversary* $\mathbf{A}$*,*

$$\mathbf{Adv}^{\mathsf{muae,icm}}_{\mathsf{CCM\_NKD}}(\mathbf{A}) \le \mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}(u, q, \tau + O(\sigma)) + \frac{q_{\mathsf{d}}}{2^t} + \frac{\sigma_{\mathsf{n}}\sigma}{2^n} + \frac{\left(d + \frac{n}{\log_2 n}\right)(p+\sigma)}{2^k} + \left(\frac{3(\log_2 n)\sigma}{2^n}\right)^{\frac{n}{\log_2 n}} + \frac{\sigma(p+\sigma)}{2^{k+n}}.$$

With a discussion similar to Section 6, dominant terms in the bounds are $\frac{q_{\mathsf{d}}}{2^t} + \frac{\sigma_{\mathsf{n}}\sigma}{2^n} + \frac{dp}{2^k}$.

7.4 Choices for PRF

As mentioned in [11, 21, 5], the concatenation of truncated BCs and CENC [16] are nice choices for the KDF in CCM_NKD. Particularly, when implementing AES with AES-NI, the KDF can be efficiently performed.

8 Authenticated Encryption with NTKD

We present an AE mode AE_NTKD that enhances the mu-security of tag-based and BC-based AE schemes including CCM and GCM by respecting its interfaces. AE_NTKD equips a nonce- and tag-based key derivation NTKD.

8.1 Parameters of AE_NTKD

Let κ, ν, and t be lengths of keys, nonce, and tags of AE_NTKD such that $t \le n$. In AE_NTKD, AD and a plaintext/ciphertext are divided into data blocks called *sectors*. Each sector is processed by using the underlying AE. Let s be the length of each sector.

8.2 The Underlying AE of AE_NTKD

Let AE be a tag-based AE scheme that is a pair of encryption and decryption algorithms $(\mathsf{AE.Enc}, \mathsf{AE.Dec})$. Let $\mathcal{K}$, $\mathcal{N}$, $\mathcal{A}$, $\mathcal{M}$, $\mathcal{C}$, and $\mathcal{T}$ be the sets of keys, nonce, AD, plaintexts, ciphertexts, and tags of AE, respectively. We define the set of tags as $\mathcal{T} := \{0,1\}^t$.

- The encryption algorithm $\mathsf{AE.Enc} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \to \mathcal{C} \times \mathcal{T}$ takes (K, N, A, M), and returns, deterministically, a pair (C, T).
- The decryption algorithm $\mathsf{AE.Dec} : \mathcal{K}\times\mathcal{N}\times\mathcal{A}\times\mathcal{C}\times\mathcal{T} \to \{\mathbf{reject}\}\cup\mathcal{M}$ takes a tuple $(K, N, A, C, \widetilde{T})$ and returns, deterministically, either the distinguished invalid symbol $\mathbf{reject} \notin \mathcal{M}$ or a plaintext $M \in \mathcal{M}$.

Algorithm 4 AE_NTKD

Encryption $\mathsf{AE\_NTKD.Enc}(K, N, A, M)$

$T_0 \leftarrow 0^t$; $\hat{N} \leftarrow \mathsf{F}^2_K(N, 0^t)$; $A_1, \ldots, A_a \xleftarrow{s} A$; $M_1, \ldots, M_m \xleftarrow{s} M$
for $i \in [a+m]$ **do**
  $\hat{K}_i \leftarrow \mathsf{F}^1_K(N, T_{i-1})$; $\hat{N}_i \leftarrow \mathsf{add}_{\mathsf{ntk}}(\hat{N}, i)$
  if $i \leq a$ **then** $(C_i, T_i) \leftarrow \mathsf{AE.Enc}(\hat{K}_i, \hat{N}_i, A_i, \varepsilon)$
    else $(C_{i-a}, T_i) \leftarrow \mathsf{AE.Enc}(\hat{K}_i, \hat{N}_i, \varepsilon, M_{i-a})$ **end if**
end for
$C \leftarrow C_1 \| \cdots \| C_m$; $T \leftarrow T_{a+m}$; **return** (C, T)

Decryption $\mathsf{AE\_NTKD.Dec}(K, N, A, C, \widetilde{T})$

$T_0 \leftarrow 0^t$; $\hat{N} \leftarrow \mathsf{F}^2_K(N, 0^t)$; $A_1, \ldots, A_a \xleftarrow{s} A$; $C_1, \ldots, C_m \xleftarrow{sn} C$
for $i \in [a+m]$ **do**
  $\hat{K}_i \leftarrow \mathsf{F}^1_K(N, T_{i-1})$; $\hat{N}_i \leftarrow \mathsf{add}_{\mathsf{ntk}}(\hat{N}, i)$
  if $i \leq a$ **then** $(M_i, T_i) \leftarrow \mathsf{AE.Enc}(\hat{K}_i, \hat{N}_i, A_i, \varepsilon)$
    else $(M_{i-a}, T_i) \leftarrow \mathsf{AE.Dec}^*(\hat{K}_i, \hat{N}_i, \varepsilon, C_{i-a})$ **end if**
end for
$M \leftarrow M_1 \| \cdots \| M_m$; $T \leftarrow T_{a+m}$
if $T = \widetilde{T}$ **then return** M **else return reject end if**

We require that

$$\begin{aligned}
&\forall (K, N, A, M), (K', N', A', M') \text{ s.t.} \\
&\qquad |M| = |M'| : |\mathsf{AE.Enc}(K, A, M)| = |\mathsf{AE.Enc}(K', A', M')|, \\
&\forall K, N, A, M : \mathsf{AE.Dec}(K, A, \mathsf{AE.Enc}(K, N, A, M)) = M.
\end{aligned}$$

$\mathsf{AE.Enc}$ and $\mathsf{AE.Dec}$ with a key $K \in \mathcal{K}$ are denoted by $\mathsf{AE.Enc}_K$ and $\mathsf{AE.Dec}_K$. Let $\mathsf{AE}_K \coloneqq (\mathsf{AE.Enc}_K, \mathsf{AE.Dec}_K)$.

We extract a tag generation function and a core function of $\mathsf{AE.Dec}$. Let $\mathsf{TagGen} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C} \to \mathcal{T}$ be the tag generation function such that for any $(K, N, A, M) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M}$, $(C, \mathsf{TagGen}(K, N, A, C)) = \mathsf{AE.Enc}(K, N, A, M)$ holds. TagGen with a key K is denoted by TagGen_K. Let $\mathsf{AE.Dec}^* : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T} \to \mathcal{M} \times \mathcal{T}$ be the core function of $\mathsf{AE.Dec}$ that produces an unverified plaintext M and a tag T, i.e., for an input $(K, N, A, C, \widetilde{T}) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T}$ to $\mathsf{AE.Dec}$, the output is defined as follows: $(M, T) \leftarrow \mathsf{AE.Dec}^*(K, N, A, C)$ and the output is M if $T = \widetilde{T}$; **reject** otherwise.

8.3 The Underlying KDF of AE_NTKD

Let $\mathsf{F} : \{0,1\}^\kappa \times \{0,1\}^\nu \times \{0,1\}^t \to \mathcal{K} \times \mathcal{N}$ be the KDF that takes a κ-bit key, nonce, and tag, and based on nonce and a tag, returns a pair of key and IV. F with a key K is denoted by F_K. For $(K, N, T) \in \{0,1\}^\kappa \times \{0,1\}^\nu \times \{0,1\}^t$, let $\mathsf{F}^1_K(N, T) \coloneqq \hat{K}$ and $\mathsf{F}^2_K(N, T) \coloneqq \hat{N}$ such that $\mathsf{F}_K(N, T) = (\hat{K}, \hat{N})$.

8.4 Specification of AE_NTKD

The specification is given in Algorithm 4 and Fig. 1. For l_{max} which is a maximum number of sectors in AD or a plaintext, let $\mathsf{add}_{\mathsf{ntk}} : \{0,1\}^\nu \times [l_{\mathsf{max}}] \to \mathcal{N}$ be a nonce-updating function that takes nonce $\hat{N}$ and a counter i, and returns nonce of the underlying AE such that $\forall \hat{N} \in \{0,1\}^\nu, i, j \in [l_{\mathsf{max}}]$ s.t. $i \neq j$: $\mathsf{add}_{\mathsf{ntk}}(\hat{N}, i) \neq \mathsf{add}_{\mathsf{ntk}}(\hat{N}, j)$. Note that in Fig. 1, $\mathsf{add}_{\mathsf{ntk}}(\hat{N}, i) = \hat{N} + (i-1)$.

$\mathsf{AE\_NTKD.Enc}_K : \{0,1\}^\nu \times \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^* \times \{0,1\}^t$ is the encryption algorithm with a key $K \in \{0,1\}^\kappa$ that takes a tuple of nonce, AD, and a plaintext, and returns a pair of a ciphertext and a tag. In $\mathsf{AE\_NTKD.Enc}$, AD and plaintext are respectively divided into sectors of s bits $A_1, \ldots, A_a$ and $M_1, \ldots, M_m$. Note that if $A = \varepsilon$, then $a = 0$. First, a nonce-based key $\hat{K}_1$ and a nonce-based IV $\hat{N}$ are defined by using the KDF F_K. Then, by iterating $\mathsf{AE.Enc}$ and F_K, AD sectors are processed, followed by the process of plaintext sectors. The KDF takes nonce N and a tag of the previous $\mathsf{AE.Enc}$ call, and returns a key of the next $\mathsf{AE.Enc}$ call.

$\mathsf{AE\_NTKD.Dec}_K : \{0,1\}^\nu \times \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^t \to \{0,1\}^* \times \{0,1\}^t$ is the decryption algorithm with a key $K \in \{0,1\}^\kappa$ that takes a tuple of nonce, AD, a ciphertext, and a tag, and returns a valid plaintext if the inputs are authenticated; the reject symbol **reject** otherwise. In $\mathsf{AE\_NTKD.Dec}_K$, AD and a ciphertext are respectively divided into sectors $A_1, \ldots, A_a$ and $C_1, \ldots, C_m$. Then, similarly to $\mathsf{AE\_NTKD.Enc}_K$, the AD sector blocks are processed by iterating $\mathsf{AE.Enc}$ and F_K, and then the ciphertext sector blocks are processed by iterating $\mathsf{AE.Dec}^*$ (instead of $\mathsf{AE.Enc}$) and F_K.

8.5 Security Definition for AE_NTKD

We consider the mu-AE security of $\mathsf{AE\_NTKD}$ in the IC model. Let u be the number of users. We use the security definition in Section 4 with the real-world oracles $\mathcal{O}_{\mathsf{real}} := ((\mathsf{AE\_NTKD}_{K^{[\omega]}})_{\omega \in [u]}, E^{\pm})$ and the ideal-world oracles $\mathcal{O}_{\mathsf{ideal}} := ((\$_\omega, \bot_\omega)_{\omega \in [u]}, E^{\pm})$, where $\forall \omega \in [u] : K^{[\omega]} \xleftarrow{\$} \{0,1\}^\kappa$ and $E^{\pm}$ is an IC. The advantage function of an adversary $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE\_NTKD}}(\mathbf{A}) := \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_{\mathsf{real}}, \mathcal{O}_{\mathsf{ideal}}}(\mathbf{A}).$$

Let p (resp. σ) be the number of offline queries (resp. BC calls of $\mathsf{AE\_NTKD}$ in online queries). Let q_{d} be the number of decryption queries. Let $\mathcal{A}$ be the set of all possible nonce-respecting computationally-unbounded adversaries with the resources.

8.6 Assumption

Regarding the KDF, we assume that F is mu-PRF secure. The definition of mu-PRF security is given in Section 7.

Regarding the underlying AE, we assume that AE is mu-AE secure in the IC model. Let u_1 be the number of users. We use the security definition given

in Section 4. In this case, we consider the following real-world and ideal-world oracles:

$$\mathcal{O}_{\mathsf{real}} \coloneqq ((\mathsf{AE}_{K^{[w]}})_{w\in[u_1]}, E^{\pm}), \qquad \mathcal{O}_{\mathsf{ideal}} \coloneqq ((\$_\omega, \bot_\omega)_{\omega\in[u_1]}, E^{\pm}),$$

where $\forall w \in [u_1] : K^{[w]} \xleftarrow{\$} \mathcal{K}$ and $E^{\pm}$ is an IC. Then, the advantage function of an adversary $\mathbf{B}$ is defined as

$$\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE}}(\mathbf{B}) \coloneqq \mathbf{Adv}^{\mathsf{dist}}_{\mathcal{O}_{\mathsf{real}},\mathcal{O}_{\mathsf{ideal}}}(\mathbf{B}).$$

Let ℓ_1 be the maximum number of primitive calls of AE per online query. Let $q_{\mathsf{d},1}$ be the number of decryption queries. Let σ_1 be the number of primitive calls of AE in all queries made by $\mathbf{B}$. Let p_1 be the number of offline queries. Let $\mathcal{Q}_1 \coloneqq (u_1, \sigma_1, q_{\mathsf{d},1}, \ell_1, p_1)$ be the query resources of adversaries. Then, for all possible computationally-unbounded adversaries with the resource $\mathcal{Q}_1$, the maximum of the advantage function is denoted by

$$\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE}}(\mathcal{Q}_1) \coloneqq \max_{\mathbf{B}} \mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE}}(\mathbf{B}).$$

In addition to the mu-AE assumption, we assume that TagGen is regular and almost universal. The definitions are given below.

Definition 2 (Regular and Almost Universal (AU)). *For an input tuple $\mathcal{D}$ to TagGen_K, let $N_{\mathcal{D}}$ be the number of primitive calls (such as BC calls and n-bit field multiplications) of $\mathsf{TagGen}_K(\mathcal{D})$. Let δ be a function that takes the number of primitive calls of TagGen_K with $\mathcal{D}_1$ and returns a probability for regular and AU.* TagGen *is said to be δ-regular if for any $Y \in \{0,1\}^t$ and any input tuple $\mathcal{D}$,*

$$\Pr[K \xleftarrow{\$} \mathcal{K}; \mathsf{TagGen}_K(\mathcal{D}) = Y] \leq \delta(N_{\mathcal{D}}, 0).$$

TagGen *is said to be δ-AU if for any distinct tuples $\mathcal{D}_1, \mathcal{D}_2$,*

$$\Pr[K \xleftarrow{\$} \mathcal{K}; \mathsf{TagGen}_K(\mathcal{D}_1) = \mathsf{TagGen}_K(\mathcal{D}_2)] \leq \delta(N_{\mathcal{D}_1}, N_{\mathcal{D}_2}).$$

8.7 mu-AE Security of AE_NTKD

The following theorem shows the mu-AE-security bound of AE_NTKD with the assumptions that F is mu-PRF secure, AE is mu-AE secure, and TagGen is regular and AU.

Theorem 3. *Let b_s be the maximum number of BC calls in* $\mathsf{AE.Enc}$ *with a pair of s-bit AD and the empty plaintext or a pair of empty AD and an s-bit plaintext. Let* TagGen *be δ-regular and δ-AU such that for the numbers of primitive calls N_1, N_2 and a positive integer c, $\delta(N_1, N_2) = \frac{c(N_1+N_2)}{2^t}$. Then, $\forall \mathbf{A} \in \mathcal{A}$:*

$$\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE\_NTKD}}(\mathbf{A}) \leq \mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}(u, \sigma, \tau + O(\sigma)) + \frac{c\sigma_{\mathsf{n}}\sigma}{b_s 2^t} + \mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE}}(\mathcal{Q}_1),$$

where $\mathcal{Q}_1$ $(= (u_1, \sigma_1, q_{\mathsf{d},1}, \ell_1, p_1)) = (\lfloor \sigma/b_s \rfloor + q, \sigma, q_{\mathsf{d}}, b_s, p)$.

Intuitively, assuming that F is mu-PRF secure and no collision occurs on the tags, we can ensure that each AE call has a fresh random key. Thus, the mu-AE security of AE_NTKD can be reduced to that of AE. The term $\frac{c\sigma_{\mathsf{n}}\sigma}{b_s 2^t}$ is the probability of the tag collision. The proof is given in Section 8.9.

8.8 Applications to CCM and GCM

We first consider AE_NTKD with CCM in the IC model, i.e., AE = CCM. Note that the parameter c of CCM is a constant [1]. Assume that $\mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}(u, \sigma, \tau + O(\sigma))$ is negligible compared with the other terms, which can be realized by using highly secure KDFs, such as BC-based PRFs [11, 21, 5, 6] and SHA-2/3-based KDFs [25, 24].

We evaluate the term $\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{CCM}}(\mathcal{Q}_1)$ with Theorem 2. Let $\mathbf{B}$ be an adversary with the resource $\mathcal{Q}_1$. Let v be the maximum number of decryption queries per user. For $w \in [u_1]$, let σ_w be the number of BC calls in queries to the w-th user. Hence, $\sigma = \sum_{w\in[u_1]} \sigma_w$. By Theorem 2, for any adversary $\mathbf{B}$, we have

$$\mathbf{Adv}^{\mathsf{muae,icm}}_{\mathsf{CCM}}(\mathbf{B}) \le \frac{q_{\mathsf{d}}}{2^t} + \sum_{w\in[u_1]} \frac{\sigma_w^2}{2^n} + \frac{\left(d + \frac{n}{\log_2 n}\right)(p+\sigma)}{2^k} + \left(\frac{3(\log_2 n)\sigma}{2^n}\right)^{\frac{n}{\log_2 n}} + \frac{\sigma(p+\sigma)}{2^{k+n}}.$$

Regarding the term $\sum_{w\in[u_1]} \frac{\sigma_w^2}{2^n}$, since the number of encryption queries to each user is at most 1 and the number of BC calls in each query is at most b_s, the term is maximum when for each of some $\lfloor q_{\mathsf{d}}/v \rfloor + 1$ users, $\mathbf{B}$ makes v decryption queries that require b_s BC calls per user. Without loss of generality, assume that the user indexes with the decryption queries is from 1 to $\lfloor q_{\mathsf{d}}/v \rfloor + 1$. In this case, for $w_1 \in [\lfloor q_{\mathsf{d}}/v \rfloor + 1]$, $\sigma_{w_1} = b_s + b_s v$, and for $w_2 \in [\lfloor q_{\mathsf{d}}/v \rfloor + 2, u_1]$, $\sigma_{w_2} \le b_s$. We thus have

$$\sum_{w\in[u_1]} \frac{\sigma_w^2}{2^n} \le (\lfloor q_{\mathsf{d}}/v \rfloor + 1) \cdot \frac{(b_s + b_s v)^2}{2^n} + \sum_{w_2 \in [\lfloor q_{\mathsf{d}}/v \rfloor + 2, u_1]} \frac{b_s \sigma_{w_2}}{2^n} \le \frac{8 b_s^2 v q_{\mathsf{d}}}{2^n} + \frac{b_s \sigma}{2^n}.$$

Regarding the number of forgery attempts v, it can be limited by rekeying. We thus assume that $v q_{\mathsf{d}} \le \sigma$, and the above bound is at most $\frac{9 b_s \sigma}{2^n}$. We then use the parameter $b_s = \sqrt{2^{n-t}\sigma_{\mathsf{n}}}$ that ensures $\frac{b_s \sigma}{2^n} = \frac{\sigma_{\mathsf{n}} \sigma}{b_s 2^t}$. Putting the bound of $\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{CCM}}(\mathbf{B})$ with $b_s = \sqrt{2^{n-t}\sigma_{\mathsf{n}}}$ into Theorem 3, the mu-AE-security bound is about

$$\frac{q_{\mathsf{d}}}{2^t} + \frac{\sqrt{2^{n-t}\sigma_{\mathsf{n}}}\sigma}{2^n} + \frac{dp}{2^k}.$$

When $t = n$, the bound ensures that AE_NTKD with CCM is mu-AE secure as long as $\sigma \le 2^n/\sqrt{\sigma_{\mathsf{n}}}$ and $p \le 2^k$.

Regarding GCM [9], Hoang et al. [13] derive the same bound for $\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{GCM}}(\mathcal{Q}_1)$ as our CCM's bound in the d-bound model. Note that GCM uses the MAC algorithm GMAC and the parameter c of GMAC is a constant. Hence, AE_NTKD with GCM is as secure as AE_NTKD with CCM regarding mu-AE security. By using $b_s = \sqrt{\sigma_{\mathsf{n}}}$ and assuming that $\mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}(u, \sigma, \tau + O(\sigma))$ is negligible and $v q_{\mathsf{d}} \le \sigma$, the mu-AE-security bound is about

$$\frac{q_{\mathsf{d}}}{2^t} + \frac{\sqrt{2^{n-t}\sigma_{\mathsf{n}}}\sigma}{2^n} + \frac{dp}{2^k}.$$

When $t = n$, AE_NTKD with GCM is mu-AE secure as long as $\sigma \le 2^n/\sqrt{\sigma_{\mathsf{n}}}$ and $p \le 2^k$.

8.9 Proof of Theorem 3

We first modify the real world, where $\mathcal{R}_\omega$ is replaced with $\mathsf{F}_{K^{[\omega]}}$ for each $\omega \in [u]$. The modified world is called "middle world." Hence, an adversary $\mathbf{A}$ interacts with the middle-world oracles $\mathcal{O}_{\mathsf{middle}} \coloneqq ((\mathsf{AE\_NTKD}[\mathcal{R}_\omega])_{\omega\in[u]}, E^{\pm})$, where $E^{\pm}$ is an IC and $\mathsf{AE\_NTKD}[\mathcal{R}_\omega]$ is $\mathsf{AE\_NTKD}_{K^{[\omega]}}$ with $\mathcal{R}_\omega$. We then have

$$\begin{aligned}\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE\_NTKD}}(\mathbf{A}) = &\left(\Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{real}}} = 1\right] - \Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{middle}}} = 1\right]\right) \\ &+ \left(\Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{middle}}} = 1\right] - \Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{ideal}}} = 1\right]\right).\end{aligned}$$

We evaluate each difference in the followings.

Upper-bounding $\Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{real}}} = 1\right] - \Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{middle}}} = 1\right]$. By the replacement from $\mathcal{O}_{\mathsf{real}}$ to $\mathcal{O}_{\mathsf{middle}}$, the difference is bounded by the mu-PRF advantage, i.e.,

$$\Pr[\mathbf{A}^{\mathcal{O}_{\mathsf{real}}} = 1] - \Pr[\mathbf{A}^{\mathcal{O}_{\mathsf{middle}}} = 1] \le \mathbf{Adv}^{\mathsf{muprf}}_{\mathsf{F}}(u, \sigma, \tau + O(\sigma)).$$

Upper-bounding $\Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{middle}}} = 1\right] - \Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{ideal}}} = 1\right]$. We use the following notations. For $\alpha \in [q]$, let m_α and a_α be the lengths m and a of the plaintext and AD in the α-th online query. For $\alpha \in [q]$, values regarding the α-th online query are denoted by using the superscript symbol of (α), e.g., $M^{(\alpha)}, C^{(\alpha)}$, etc. Let u_α be the user index of the α-th online query.

We next define the following collision events in the middle world. For $\alpha \in [q]$ and $i \in [a_\alpha + m_\alpha]$, let $\mathcal{D}_i^{(\alpha)}$ be a pair of an AD sector and a ciphertext sector at the i-th AE call of the α-th online query. If $i \le a_\alpha$, then $\mathcal{D}_i^{(\alpha)} = (A_i^{(\alpha)}, \varepsilon)$; if $i > a_\alpha$, then $\mathcal{D}_i^{(\alpha)} = (\varepsilon, M_{i-a_\alpha}^{(\alpha)})$.

$$\begin{aligned}\mathsf{coll} \Leftrightarrow \exists \alpha, \beta \in [q], i \in [a_\alpha + m_\alpha], j \in [a_\beta + m_\beta] \text{ s.t. } &(\alpha, i) \neq (\beta, j) \\ &\wedge \mathsf{u}_\alpha = \mathsf{u}_\beta \wedge N^{(\alpha)} = N^{(\beta)} \\ &\wedge (T_{i-1}^{(\alpha)}, \mathcal{D}_i^{(\alpha)}) \neq (T_{j-1}^{(\beta)}, \mathcal{D}_j^{(\beta)}) \wedge T_i^{(\alpha)} = T_j^{(\beta)}.\end{aligned}$$

The collision event considers a tag collision of some two distinct sectors or keys, yielding a key collision of the underlying AE. In other worlds, each key of the AE is independently chosen as long as coll does not occur. With the event, we have

$$\begin{aligned}\Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{middle}}} = 1\right] - \Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{ideal}}} = 1\right] \le &\Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{middle}}} = 1 \mid \neg\mathsf{coll}\right] \\ &- \Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{ideal}}} = 1\right] + \Pr[\mathsf{coll}].\end{aligned}$$

Upper-bounding $\Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{middle}}} = 1 \mid \neg\mathsf{coll}\right] - \Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{ideal}}} = 1\right]$. We give an overview of the evaluation. The detail evaluation is given in the full version of this paper [22].

Assume that coll does not occur. In the nonce-respecting setting, all keys of AE.Enc in the middle world are independently chosen by RFs $(\mathcal{R}_\omega)_{\omega\in[u]}$. Hence, $\{\mathsf{AE\_NTKD.Enc}[\mathcal{R}_\omega]\}_{\omega\in[u]}$ behave as random-bit oracle up to the advantage $\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE}}(\mathcal{Q}_1)$, where $\mathcal{Q}_1 = (\lceil\sigma/b_s\rceil + q, \sigma, q_{\mathsf{d}}, b_s, p)$. Moreover, each tag of AE_NTKD.Dec in the middle world is defined by using AE.Dec. Hence, the probability of forging a tag of $\mathsf{AE\_NTKD.Dec}[\mathcal{R}_\omega]$ is bounded by the advantage $\mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE}}(\mathcal{Q}_1)$. We thus have

$$\Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{middle}}} = 1 \mid \neg\mathsf{coll}\right] - \Pr\left[\mathbf{A}^{\mathcal{O}_{\mathsf{ideal}}} = 1\right] \le \mathbf{Adv}^{\mathsf{muae}}_{\mathsf{AE}}(\mathcal{Q}_1).$$

Upper-bounding Pr[coll]. For each $\alpha,\beta \in [q], i \in [a_\alpha + m_\alpha], j \in [a_\beta + m_\beta]$ such that $(\alpha, i) \neq (\beta, j)$, $\mathsf{u}_\alpha = \mathsf{u}_\beta$ and $N^{(\alpha)} = N^{(\beta)}$, if $T^{(\alpha)}_{i-1} \neq T^{(\beta)}_{j-1}$, then the keys $\hat{K}^{(\alpha)}_i$ and $\hat{K}^{(\beta)}_j$ are independently chosen, and thus by the regular property of TagGen, the probability of the tag collision $T^{(\alpha)}_i = T^{(\beta)}_j$ is at most $\frac{cb_s}{2^n}$. If $T^{(\alpha)}_{i-1} = T^{(\beta)}_{j-1}$ and $\mathcal{D}^{(\alpha)}_i \neq \mathcal{D}^{(\beta)}_j$, then by the AXU or regular property of TagGen, the probability of the tag collision is at most $\frac{2cb_s}{2^n}$.

For $\omega \in [u]$, let N_ω be the number of distinct nonces in queries to the ω-th user. For $i \in [N_\omega]$, let $\sigma_{\omega,i}$ be the number of BC calls in online queries with the i-th nonce to the ω-th user. Then, for each $i \in [N_\omega]$, there are at most $\lceil\frac{\sigma_{\omega,i}}{b_s}\rceil$ keys of AE. By using the above bounds, we have

$$\begin{aligned}
\Pr[\mathsf{coll}] &\le \sum_{\omega\in[u], i\in[N_\omega]} \binom{\lceil\frac{\sigma_{\omega,i}}{b_s}\rceil}{2} \cdot \frac{2cb_s}{2^t} \\
&\le \sum_{\omega\in[u], i\in[N_\omega]} \frac{0.5(\lceil\frac{\sigma_{\omega,i}}{b_s}\rceil)^2 \cdot 2cb_s}{2^t} \\
&\le \sum_{\omega\in[u], i\in[N_\omega]} \frac{4c(\sigma_{\omega,i}/b_s)^2 \cdot b_s}{2^t} \\
&\le \frac{4c\sigma_{\mathsf{n}}\sigma}{b_s 2^t}.
\end{aligned}$$

Conclusion of the Proof. Combining the above bounds, we obtain the bound in Theorem 3.

■ (Theorem 3)

References

1. Bellare, M., Pietrzak, K., Rogaway, P.: Improved Security Analyses for CBC MACs. In: CRYPTO 2005. LNCS, vol. 3621, pp. 527–545. Springer (2005)

2. Bellare, M., Tackmann, B.: The Multi-user Security of Authenticated Encryption: AES-GCM in TLS 1.3. In: CRYPTO 2016. LNCS, vol. 9814, pp. 247–276. Springer (2016)
3. Biham, E.: How to Decrypt or Even Substitute DES-Encrypted Messages in 2^{28} Steps. Inf. Process. Lett. **84**(3), 117–124 (2002)
4. Black, D.L., McGrew, D.A.: Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol. RFC **5282**, 1–19 (2008)
5. Bose, P., Hoang, V.T., Tessaro, S.: Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds. In: EUROCRYPT 2018. LNCS, vol. 10820, pp. 468–499 (2018)
6. Cogliati, B., Jha, A., Nandi, M.: How to Build Optimally Secure PRFs Using Block Ciphers. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020. LNCS, vol. 12491, pp. 754–784. Springer (2020)
7. Degabriele, J.P., Govinden, J., Günther, F., Paterson, K.G.: The Security of ChaCha20-Poly1305 in the Multi-User Setting. In: CCS 2021. pp. 1981—2003. ACM (2021)
8. Dworkin, M.: NIST Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality. `https://csrc.nist.gov/pubs/sp/800/38/c/upd1/final` (2007)
9. Dworkin, M.: NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. `https://csrc.nist.gov/pubs/sp/800/38/d/final` (2007)
10. Dworkin, M.: NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. `https://csrc.nist.gov/pubs/sp/800/38/b/upd1/final` (2016)
11. Gueron, S., Lindell, Y.: Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation. In: CCS 2017. pp. 1019–1036. ACM (2017)
12. Günther, F., Thomson, M., Wood, C.A.: Usage Limits on AEAD Algorithms. `https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-aead-limits-07` (2023)
13. Hoang, V.T., Tessaro, S., Thiruvengadam, A.: The Multi-user Security of GCM, Revisited: Tight Bounds for Nonce Randomization. In: CCS 2018. pp. 1429–1440. ACM (2018)
14. Housley, R.: Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP). RFC **4309**, 1–13 (2005)
15. ISO: Iso/iec 19772:2020 information security—authenticated encryption (2020)
16. Iwata, T.: New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In: FSE 2006. LNCS, vol. 5665, pp. 67–83. Springer (2006)
17. Jonsson, J.: On the Security of CTR + CBC-MAC. In: Selected Areas in Cryptography, SAC 2002. LNCS, vol. 2595, pp. 76–93. Springer (2002)
18. Kampanakis, P., Campagna, M., Crocket, E., Petcher, A.: Practical challenges with aes-gcm and the need for a new mode and wide-block cipher. presented at NIST The Third NIST Workshop on Block Cipher Modes of Operation 2023, `https://csrc.nist.gov/Presentations/2023/practical-challenges-with-aes-gcm` (2023)
19. Luykx, A., Mennink, B., Paterson, K.G.: Analyzing Multi-key Security Degradation. In: ASIACRYPT 2017. LNCS, vol. 10625, pp. 575–605. Springer (2017)
20. McGrew, D.A., Bailey, D.V.: AES-CCM Cipher Suites for Transport Layer Security (TLS). RFC **6655**, 1–8 (2012)

21. Naito, Y.: Tweakable Blockciphers for Efficient Authenticated Encryptions with Beyond the Birthday-Bound Security. IACR Trans. Symmetric Cryptol. **2017**(2), 1–26 (2017)
22. Naito, Y., Sasaki, Y., Sugawara, T.: Tight Multi-User Security of CCM and Enhancement by Tag-Based Key Derivation Applied to GCM and CCM. IACR Cryptol. ePrint Arch. p. 953 (2025)
23. National Institute of Standards and Technology: Pre-Draft Call for Comments: GCM and GMAC Block Cipher Modes of Operation. https://csrc.nist.gov/pubs/sp/800/38/d/r1/iprd (2025)
24. NIST: Fips pub. 198-1: The keyed-hash message authentication code (hmac). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf (2008)
25. NIST: Fips pub. 202: Sha-3 standard: Permutation-based hash and extendable-output functions). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf (2015)
26. Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.3. RFC **8446**, 1–160 (2018)
27. Rescorla, E., Tschofenig, H., Modadugu, N.: The Datagram Transport Layer Security (DTLS) Protocol Version 1.3 – draft-ietf-tls-dtls13-43. https://tools.ietf.org/html/draft-ietf-tls-dtls13-43 (2021)
28. Rogaway, P., Wagner, D.A.: A Critique of CCM. Cryptology ePrint Archive, Paper 2003/070 (2003)
29. Salowey, J.A., McGrew, D., Choudhury, A.: AES Galois Counter Mode (GCM) Cipher Suites for TLS. RFC **5288**, 1–8 (2008)
30. Seaman, M.: IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security. https://ieeexplore.ieee.org/document/8585421 (2018)
31. Thomson, M., Turner, S.: Using TLS to Secure QUIC. RFC **9001**, 1–52 (2021)
32. Viega, J., McGrew, D.: The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH. RFC **4543**, 1–14 (2006)
33. Whiting, D., Housley, R., Ferguson, N.: IEEE P802.11 Wireless LANs: AES Encryption & Authentication Using CTR Mode & CBC-MAC. https://mentor.ieee.org/802.11/dcn/02/11-02-0001-02-000i-aes-encryption-authentication-using-ctr-mode-with-cbc-mac.doc (2002)
34. Whiting, D., Housley, R., Ferguson, N.: Counter with CBC-MAC (CCM). RFC **3610**, 1–26 (2003)
35. Wi-Fi Alliance: WPA3 Specification Version 3.2. https://www.wi-fi.org/system/files/WPA3\%20Specification\%20v3.2.pdf (2023)
36. Woolley, M.: Bluetooth core specification version 5.4 (2023)
37. Zhang, X., Shen, Y., Wang, L.: Multi-User Security of CCM Authenticated Encryption Mode. In: CCS 2024. pp. 4331–4345. ACM (2024)
38. ZigBee Alliance, Inc.: Zigbee specification. https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf (2015)